A Self-Assessment Method for Organizational Awareness 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.kaberuka1}@nottingham.ac.uk; m.bada@qmul.ac.uk

Abstract

The adoption of Security by Design offers a means to significantly reduce the persistent challenge posed by the exploitation of systems and devices that are deployed with inherent vulnerabilities. However, the path to widespread use of technologies based upon these principles can face barriers to adoption at the organizational level. Organizations need to recognize their own need for protection, and to understand that they could be better served by enhanced technologies. Recognizing that many are likely to need help in addressing this need, this paper presents a comprehensive Organizational Self-Assessment Methodology which aims at enhancing digital security through proactive measures. By capturing a diverse range of organizational data, this methodology offers a holistic view of technology usage and existing security practices within an organization. Through the visualization of assessment outputs, stakeholders gain valuable insights into areas for improvement and potential vulnerabilities. The paper outlines the basis of the assessment methodology, and illustrates the resulting visualizations that organizations would be able to obtain. Moreover, the development of a Self-Assessment Tool to streamline data collection and analysis, ultimately empowering organizations to bolster their digital security posture, is discussed.

Introduction

It is increasingly recognized that cybersecurity needs to be built-into our technologies (security by *design*) and be their standard operating mode (security by *default*). Experience has repeatedly shown that an absence of such attention can lead to exploitable vulnerabilities, which then become embedded within deployed technologies and are difficult to address at a later stage. The Security by design paradigm advocates addressing security from the outset and is particularly relevant to the hardware context. However, prior stakeholder engagement (Benson et al., 2021) has established that awareness of hardware security aspects can be limited during technology adoption, which may mean that decisions are made without due consideration and understanding.

Most decision-makers are now aware of cyber security and would even claim it as a priority. For example, the UK Cyber Security Breaches Survey reports that 71% of respondents from the 1,700+ organizations surveyed considered that their directors, trustees, and other senior managers considered security to be a very high or fairly high priority (DSIT, 2023). 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. However, 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.

This paper builds upon previous work investigating organization awareness of Digital Security by Design (DSbD) and the potential acceptance of the concept as the basis for future technology procurement and deployment (Furnell et al. 2023). The findings of the initial investigation had revealed that while the generally positive perspective prevails around the potential to adopt to secure technology, there was a relatively limited awareness of DSbD itself, as well as challenges to be faced in promoting the adoption in practice. The findings have been used to support the design of a self-assessment method, which aims to allow organizations to profile their environment in terms of factors that would motivate DSbD adoption, and potential opportunities for incorporating it within their environment. The approach provides the basis for a resulting Self-Assessment Tool that enables the data collection, collation and analysis in practice.

Background

In the UK, the National Cyber Security Centre (NCSC), promotes the importance of building security into hardware and software components from the ground up, and advocates a resulting set of Secure by Default principles 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.

Based upon a similar ethos, 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). This provides fine-grained hardware-enforced access protection of objects in memory, and programs using capabilities are generally incapable of making out-of-bounds accesses. Given that Microsoft have previously suggested that "~70% of the vulnerabilities addressed through a security update each year continue to be memory safety issues" (Miller, 2019), the ability to avoid these issues offers the promise of significant reductions in related security issues and exploits. 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 and enables partners in the DSbD initiative to test the new architecture in practical cases.

While the advancements of CHERI and Morello deliver a technical foundation, this alone is no guarantee that the approach will be adopted by technology developers and manufacturers (for whom it can represent a significant departure). History reveals numerous examples of good technologies that were not successful (Adner and Kapoor, 2016), and so simply providing a viable DSbD solution is not sufficient. In recognition of this, a further initiative, the Digital Security by Design Social Science Hub+ (Discribe – see www.discribehub.org), was established within the wider DSbD program to apply social and economic science to the adoption of new secure technologies. Discribe's resulting focus includes examination of:

- 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 research presented here is linked to the first aspect and the project is seeking to support organizations in terms of:

- recognizing and assessing where DSbD is relevant to them, and whether it would be cost-effective;
- providing a measure of organizational 'DSbD readiness', based on assessing 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.

In an ideal world, all participants in the business would all be aligned in their understanding of and support for cybersecurity. In practice, the pursuit of security will depend upon potentially varying levels of knowledge and competing priorities from different parts of the business (e.g. with two thirds of the respondents from the authors' prior survey having cited this as a challenge). As such, there is a need for related consultation with organizational stakeholders, and the next section proceeds to discuss the design of an approach that enables assessment of DSbD awareness and readiness within their own environments.

An Organizational Self-Assessment Methodology

The assessment is based upon the capture of a range of supporting data from across the organisation, with the aim of building a picture of how technology is used, and how security has already been approached and experienced. Other approaches look at economics of cybersecurity investment (Gordon and Loeb, 2002). However, the organization may not even get to that stage if those involved have not bought into the idea in the first place.

Assessment questions

The assessment aims to capture a breadth of information about how security is viewed, the current security posture of the organisation, and the consequent potential for investment and adoption of enhanced technologies. The resulting assessment categories are summarised in Table 1. Moreover, this is approached from the perspective of different key stakeholders who could influence the resulting decisions. It is important to note that the approach is relatively lightweight in the extent to which it directly queries stakeholders in relation to the DSbD concept itself. The rationale here is that DSbD is not well-recognised in the wider community and so there would be little value in asking for stakeholder views around a technology that does not yet exist and of which they will have had no experience. As such, the method focuses on questions that reveal the related attitudes in other ways.

To expand further upon the resulting ratings proposed in the final column, the nature and rationale for each is defined as follows:

- The *Need*-related categories (TDU and IAB) provide a foundation for understanding why security is relevant to the organization. While the IT/security staff may be seen as the most likely source(s) from which to obtain authoritative / factual responses, collecting related information from different stakeholder sources provides a means to determine whether the perception/understanding is consistent across different business functions.

- The *Attitude*-related categories represent the most significant aspect of data collection in terms of indicating what an organization is likely to do in terms of security and related decision-making. One would naturally expect the security-focused stakeholder group to exhibit the most positive perspective, and the interesting aspect is then to determine how their stance compares to that of the other groups. In practice, although they would also be categorized as 'technical' stakeholders, even the CIO group may be less supportive of security than their CISO colleagues (e.g. on the basis that their main priority may be to deliver the IT services *effectively*, whereas the CISO will be keen to ensure that they are delivered *securely*) (Red Helix, 2023) and so there may be an inherent tension in their respective positions (Ottolenghi, 2021) that the assessment would help to identify and characterise.
- The *Awareness*-related category is more focused on appetite to adopt DSbD-based technologies as the opportunities emerge. Most of the underlying questions can still survey the full range of stakeholders in order to assess the alignment of the business as a whole. However, in organisations producing their own technology products, it is also relevant to ask the CEO and technical stakeholders more specifically about their awareness of and adherence to the secure-by-design principles.

Table 1: 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 organisation is using the technology for, its dependence upon it, etc.	Inform a 'Need' rating
Incidents and Breaches (IAB)	10	Highlights the organisation'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 organisation as a whole.	Inform an '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 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

The resulting data collection is based upon a set of 47 questions, and a full list of these is presented in the Appendix. However, the number of questions that an assessment would involve in practice depends upon the stakeholder concerned, and the nature of their responses. There are also certain questions that are only asked in cases where the organisation 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).

When an assessment is conducted via a supporting tool, each question will offer an optional 'comments' box should the respondents require a means to explain/contextualize their answer , and each overall *section* will also have a comments area in case it is useful to record a more general/overall comment across the set of questions (e.g. a given stakeholder may wish to give a sense of how authoritative or otherwise they might consider their responses to be).

Stakeholder perspectives

Given that the aim of the approach (and the resulting tool) is to assess *organizational* readiness, it is important to consider the multiple perspectives that would be expected influence this. As such, a key aspect is to capture related views from different segments of the business, recognizing that different stakeholders are likely to have different perspectives and perceptions in relation to the security issues to be addressed and how these compare to other business priorities. As a result, consideration is being given to five stakeholder perspectives as indicated in Table 2. 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 categorised as business or technically focused, which may be relevant groups to compare in terms of the responses in various aspects of the assessments.

Table 2: Stakeholder types to involve in data collection

Stakeholder		**Description**
Business	CEO	Representing the senior leadership perspective, and likely to be setting the overall tone and priority towards cybersecurity for the organisation. Depending upon the organisation, the actual role may be Managing Director, or similar.
	CFO	Representing the finance perspective, which is significant in ensuring that cyber security receives sufficient resource and prioritisation to enable investment to happen.
	CPO	Representing the procurement / purchasing perspective, which is relevant when considering the influence on when, where and how new technology investments are realised.
Technical	CIO	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.
	CISO	Representing the responsibility for cyber security provision and decision making. Depending upon the size of the organisation, this stakeholder function may not be distinct from the CTO position.

The collection phase obtains weighted data points from these different stakeholders in order to assess their respective awareness, understanding and acceptance of related security needs and investment. It also provides a basis to assess the extent to which the organization may benefit from DSbD based upon its activities and prior experience of security incidence.

In terms of audience applicability, it is considered that (by default) there is value in posing most of the questions to all audiences, unless they are not involved at all and/or lack the background to comment. Consequently, the Table in the Appendix indicates that most questions would be presented to all stakeholders.

Conducting Assessments

Organizations should be able to configure to various aspects of how they utilize the method. For example, they may not have distinct representatives for all the stakeholder roles listed in Table 2, and so would need the opportunity to indicate which ones they have and who holds the position. They may also wish to assign alternative weights to some of the questions and to vary the frequency of assessments to best match their business, purchasing and technology-refresh cycles.

Given the range of stakeholder perspectives involved, it is considered that the approach is likely to be more meaningful in medium and large organisations. Small, and particularly micro, organisations would be unlikely to have distinct stakeholders in the same way, and indeed several aspects could conceivably be held by the same role (or indeed the same individual) – thereby reducing the need/relevance of conducting an assessment to triangulate across different perspectives.

As a baseline in practice, the assessment would seem relevant to undertake in the event of there being at least three distinct stakeholder perspectives to be gained, and for these to be distributed across the technical and non-technical constituencies.

Visualization of Assessment Outputs

Once the assessment data has been fully collected, there are two key requirements in terms of the visualization:

- To compare and contrast different stakeholder (or stakeholder group) perspectives against each other in order to determine the extent of alignment and compatibility between them.
- To track the evolution of a given stakeholder perspective over time (i.e. to give a sense of whether the organization is advancing, maintaining or retracting its position).

To provide an illustration of how this would work in practice, we use question DSA7 from the *DSbD-Specific Awareness* category, which asks stakeholders "*What obstacles would you face if migrating from your current technology to secure by design devices*?". This offers the following options as answers:

- None
- Don't know
- Limited budget/resources
- Lack of awareness/understanding of security risks
- Difficulty in prioritizing security investments against other competing priorities
- Lack of executive support and commitment
- Inadequate expertise and skills in managing security investments
- Time and effort required
- Disruption to current operations and processes
- Compatibility with existing systems
- uncertainty about the benefits
- Resistance to change
- Other (please specify)

On each occasion that a self-assessment is performed, each stakeholder will provide one set of responses to the question. Therefore, a meaningful visualization needs to have a way of showing *who* selected *which* options. To this end, Figures 1 to 3 illustrate the potential for alternative visualizations of the same dataset, using an example of the types of responses that could be received from across the different stakeholders. The first example, in Figure 1, is ordered by 'obstacle type' and indicates which stakeholder responded against each one).

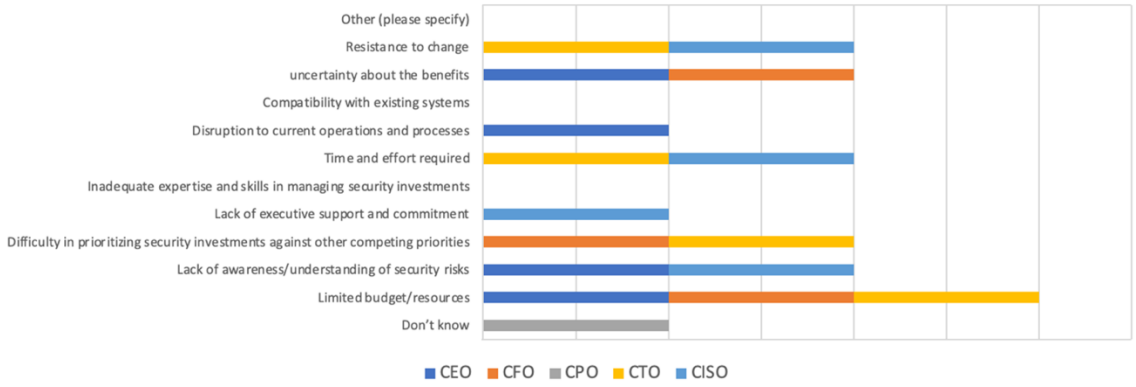

Figure 1: Visualization by response type

An alternative view of the same data is shown in Figure 2, which orders it by stakeholder type instead and shows which obstacles each party had perceived.

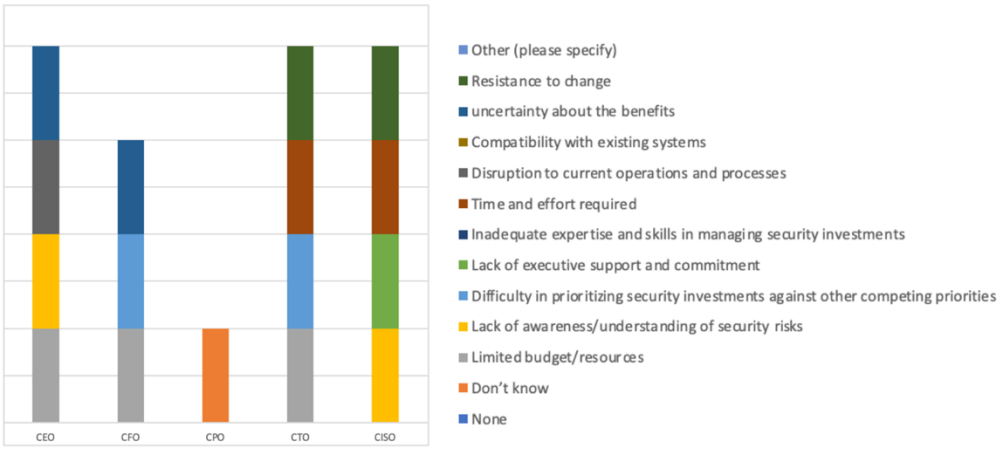

Figure 2: Visualization by stakeholder type

Departing from the use of stacked charts, a third visualization is offered in Figure 3, this time adopting a matrix-based approach, which is arguably the easiest basis from which to determine who said what, but loses the more overtly visual aspect of the charts). In the case of these particular visualizations it is clear that there is some disparity between the responses as a whole, but equally some alignment between certain stakeholders in relation to individual issues. It is also clear that in this case the CPO is an outlier compared to their colleagues, and so could benefit from some further awareness-raising in this area.

Constraints	Stakeholders				
	CEO	CFO	CPO	CTO	CISO
None					
Don't know			✓		
Limited budget/resources	✓	✓		✓	
Lack of awareness/understanding of security risks	✓				✓
Difficulty in prioritizing security investments competing priorities		✓		✓	
Lack of executive support and commitment					✓
Inadequate expertise and skills in managing security investments					
Time and effort required				✓	✓
Disruption to current operations and processes	✓				
Compatibility with existing systems					
Uncertainty about the benefits	✓	✓			
Resistance to change				✓	✓
Other					

Figure 3: Matrix-based visualization example

In terms of tracking over time, this lends itself to look from the perspective of individual stakeholders, or the average across groups (e.g. business or technical) for the organization as a whole. As an example, Figure 4 takes the same stakeholder (here a CEO) and then shows how/if their position changes from assessment to assessment (with the result in this case suggesting that their perception of challenges is increasing as time goes on).

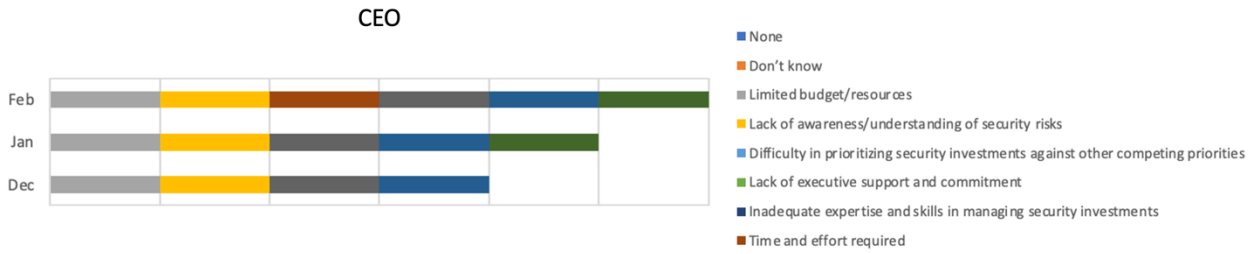

Figure 4: Tracking assessment results over time

In addition to assessing the results for individual issues across multiple stakeholders and over time, there will also be potential for more detailed levels of reporting based upon queries that draw across multiple data points. For example:

- Do the Attitude factors align with the findings from the Need results, and is this consistent across the stakeholder groups?
- Does the overall resilience score of the organisation align with the prioritisation of security across the stakeholder groups?
- Does the willingness to adopt new security technologies agree with the factors described as influencing adoption of any new security technologies?
- Does familiarity with the concept of Digital Security by Design (DSbD) influence willingness to adopt new security technologies across the stakeholder groups?

An automated tool is needed to collect the data from the different stakeholders, conduct thorough analysis, and offer user-friendly reporting in an accessible manner. Such a tool can automate the intricate processes involved in collecting diverse security-related data and presenting the findings in a format that is easily understandable and accessible to stakeholders. Steps toward the realization of such a tool are therefore discussed in the next section.

Towards a Self-Assessment Tool

The implementation of the accompanying Self-Assessment Tool (SAT) is work-in-progress at the time of writing, but this section gives an insight into how the approach is expected to be automated and assisted in terms of both the data collection and subsequent analysis.

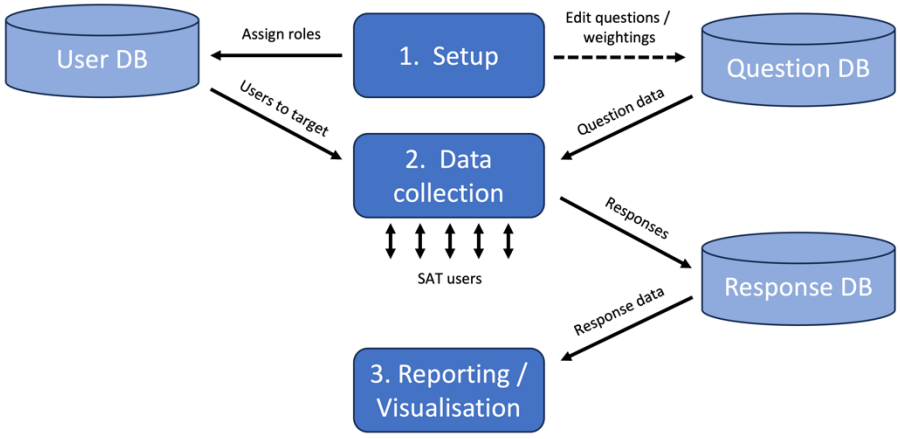

Figure 5: Self-Assessment Tool deployment process

The overall process from the perspective of the SAT administrator (i.e. the individual in overall control of it for the organization) would be as depicted in Figure 5, and outlined below:

- **Initial Setup:** The process needs to start by characterizing the organization. This includes determining which of the stakeholder roles used by the SAT exist within the organization and who covers them, in order to determine the responses required and which questions get assigned to whom. It is also relevant to indicate whether the organization is completing their assessment as a technology consumer or producer.
- **Data Collection:** A process that is run for each identified stakeholder, with users logging in providing responses for the role against which they have been registered. The data collection will occur via a questionnaire-style interface that enables users to see the broad areas of enquiry, their progress (both overall and within the current theme), and offers an option to save and resume later. A mock-up of a related interface is shown in Figure 6. The 'administrator' of the SAT within the organization should have oversight of the progress of data collection as a whole, including the status of each of the other users.
- **Reporting and visualization:** Further interfaces are required for the visualization and reporting aspects. In addition to the representation of data from individual questions (as illustrated in the previous section), another form of output would be an organizational 'Scorecard', denoting their security need (e.g. based on what they do and any incidents experienced), posture (e.g. based on use of safeguards) and attitude (e.g. based upon priority, investment etc). Each element would have a rating, derived from combining the different stakeholder inputs. In utilizing the data for such scoring, it is considered that the SAT could usefully allow weighting of data points from different stakeholders (e.g. CISO, CFO, etc)– i.e. to enable certain stakeholders to have more influence in the calculations for certain measures. For example, it may be relevant for scoring around IAB questions to be weighted heavily towards responses from the CISO, who will typically be better placed to know the details of prior incidents than (for example) the CEO or CPO.

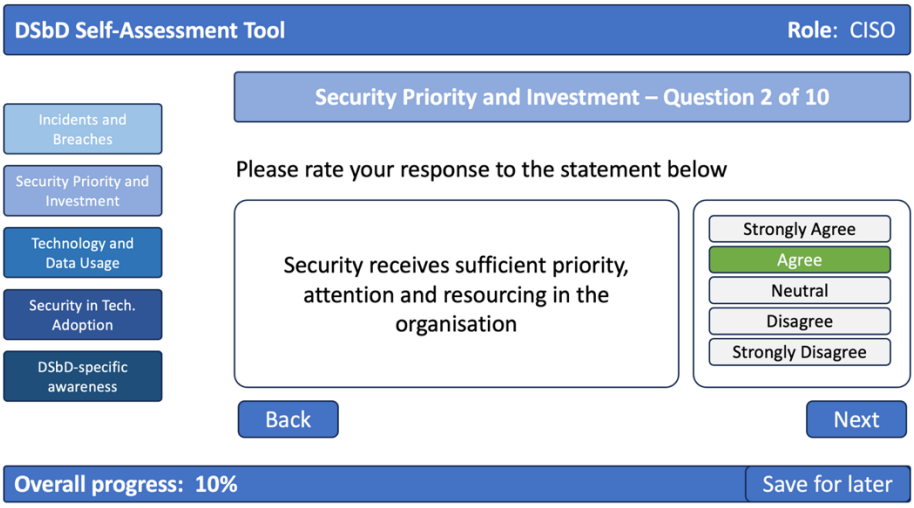

Figure 6: Example of SAT data collection approach

In terms of conducting assessments, organisations ought to be able to re-run their assessments on a selective basis by section and/or by role-holder, rather than needing to re-run the process in its entirety. Older assessments should be archived to track progression (i.e. by re-running the process, the organization could see if their scorecard changes over time, and so maintaining a record/history of earlier scores and dates would be relevant).

An organization would typically launch a SAT run that all stakeholders would then be requested to participate in. However, it would also be valid to do *partial* runs in particular circumstances. For example, this could include individual assessments of technical and non-technical subsets to see if they are aligned, or assessments focused on particular stakeholders that were previously outliers in a prior full run.

Conclusions

In conclusion, the method described provides the basis for the implementation of an accompanying Self-Assessment Tool, which holds immense potential in bolstering organizational cybersecurity efforts. 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.

By leveraging relevant tools and methodologies, organizations can enhance their resilience against evolving cyber risks and ensure the protection of sensitive data and critical infrastructure. Embracing this proactive approach is key to staying ahead of emerging threats and maintaining a robust cybersecurity posture in today's dynamic threat landscape.

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.

References

Adner, R. and Kapoor, R. (2016). Innovation ecosystems and the pace of substitution: Re-examining technology S-curves. *Strategic Management Journal*. Vol. 37, No. 4, pp625-648.

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.

DSbD. (2024). "About Digital Security by Design", Digital Security by Design. https://www.dsbd.tech/about/ (accessed 25 February 2024).

DSIT. (2023). Cyber security breaches survey 2023 - Official Statistics. Department for Science, Innovation & Technology. 19 April 2023. https://www.gov.uk/government/statistics/cyber- security-breaches-survey-2023/cyber-security-breaches-survey-2023

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

Gordon, L.A. and Loeb, M.P. (2002). The economics of information security investment. *ACM Transactions on Information and System. Security*. Vol. 5, No. 4, pp438–457.

Miller, M. 2019. "Trends, Challenges, and Strategic Shifts in the Software Vulnerability Mitigation Landscape", Microsoft Security Response Center, 7 February 2019. https://msrnd-cdn-stor.azureedge.net/bluehat/bluehatil/2019/assets/doc/Trends%2C%20Challenges%2C%20and%20Strategic%20Shifts%20in%20the%20Software%20Vulnerability%20Mitigation%20Landscape.pdf

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

Ottolenghi, L. (2021). The intertwined CIO/CISO relationship and why it matters, *CXO REvolutionaries*, 16 August 2021. https://www.zscaler.com/cxorevolutionaries/insights/intertwined-ciociso-relationship-and-why-it-matters

Red Helix. (2023). CIO/CISO Conflicting Priorities. 16 March 2023. https://www.redhelix.com/media/cio-ciso-conflicting-priorities/

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

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

Vachon, P. (2024). Security Mismatch, *Communications of the ACM*, Vol. 67, No. 2, pp40-41.

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" https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201406-isca2014-cheri.pdf

Appendix – Assessment Questions

The list below presents the full set of questions that support the assessment methodology. Each has a reference code indicating the parent category and its sequence within it. The list also shows the default set of stakeholders to whom it is suggested that the questions would be posed. The P column flags those questions that only apply to organisations that Produce their own products/technologies.

Each question has an associated rationale and response types (e.g. multiple choice, multiple selection), but in the interests of space these are not presented here.

Ref.	Question	P	Audience				
			CEO	CFO	CPO	CISO	CIO CTO
TDU1	Which of the following technologies are *utilised* within your organisation (i.e. they are in use somewhere to some extent)?		✓	✓	✓	✓	✓
TDU2	How would you rate your organisation's overall dependence upon IT devices?		✓	✓	✓	✓	✓
TDU3	Which of the following technologies do you believe are *critical* within your organisation (i.e. day-to-day operations *depend* upon them)?		✓	✓	✓	✓	✓
TDU4	Which of the following types of data is stored and processed on your organisation's devices?		✓	✓	✓	✓	✓
TDU5	How would you rate your overall resilience to technology-based disruption?		✓	✓	✓	✓	✓
TDU6	Devices currently deployed in the organisation are protected from security vulnerabilities and breaches?					✓	✓
IAB1	Direct prior experiences of security incidents or breaches have increased your organisation's *need* for cybersecurity measures.		✓	✓		✓	✓
IAB2	Reporting of incidents and breaches within other organisations has increased your own attention towards cybersecurity.		✓	✓		✓	✓
IAB3	Which of the following do you believe that your organisation has *experienced in the last 12 months*?		✓	✓		✓	✓
IAB4	Which of the following are you most *concerned* about?		✓	✓		✓	✓
IAB5	Has your organisation experienced any incidents that you would link directly to the exploitation of hardware-based vulnerabilities?					✓	✓
IAB6	Has your organisation experienced any incidents that you would link directly to the exploitation of software-based vulnerabilities?					✓	✓
IAB7	The organisation would be interested in implementing more secure technologies that would reduce exploitation-based security breaches.					✓	✓
IAB8	To what extent are you aware of any instances of own products being compromised?	Y	✓			✓	✓
IAB9	What effect has awareness of incidents and breaches had upon your organisation's priority towards cybersecurity in budgeting and financial planning?		✓	✓		✓	✓

IAB10	The organisation has invested more in cybersecurity as a direct response to prior incidents or breaches.		✓	✓		✓	✓
SPI1	Security is a high priority for our organisation		✓	✓	✓	✓	✓
SPI2	Security receives sufficient attention and resourcing in the organisation		✓	✓	✓	✓	✓
SPI3	Approximately what proportion of your organisations IT budget do you estimate is allocated to cyber security?		✓	✓	✓	✓	✓
SPI4	Security receives a sufficient level of upper management support.		✓	✓	✓	✓	✓
SPI5	What factors drive your security investments?		✓	✓	✓	✓	✓
SPI6	What challenges does your organisation face in driving security investments?		✓	✓	✓	✓	✓
SPI7	Other parts of the organisation recognise and prioritise security to the same extent as you?		✓	✓	✓	✓	✓
SPI8	The organisation would review its security investments in response to changes in available controls and safeguards?		✓	✓	✓	✓	✓
SPI9	The organisation would review its security investments in response to changes in the threat landscape?		✓	✓	✓	✓	✓
SPI10	To what extent would you be willing to invest in new/additional technology adoption to improve cyber security?		✓	✓	✓	✓	✓
STA1	What factors should influence the adoption of any new security technologies?		✓	✓	✓	✓	✓
STA2	When purchasing new technology for *general use*, how much more would the organisation be prepared to spend for a 'more secure' device?		✓	✓	✓	✓	✓
STA3	When purchasing new technology for *critical systems*, how much more would the organisation be prepared to spend for a 'more secure' device?		✓	✓	✓	✓	✓
STA4	Rate the relative importance of the following factors in the context of your technology investments: Security, Cost, Usability		✓	✓	✓	✓	✓
STA5	When considering technology device purchases, how would you rate your organisation's priority?		✓	✓	✓	✓	✓
STA6	How important are manufacturer/vendor security assurances when procuring new devices?		✓	✓	✓	✓	✓
STA7	Manufacturer/vendor security assurances are evaluated when procuring new devices?		✓	✓	✓	✓	✓
STA8	How would you rate the resilience of your current devices against hardware vulnerabilities?					✓	✓
STA9	Improving security justifies additional effort/cost to integrate it within our products?	Y	✓	✓		✓	✓
STA10	Do you promote security as a relevant feature of your own product(s)?	Y	✓	✓		✓	✓
STA11	Do you believe that the security aspects of your product(s) are important to customers?	Y	✓	✓		✓	✓

DSA1	How familiar are you with the concept of Digital Security by Design (DSbD), which promoted secure-by-design principles in technology development?		✓	✓	✓	✓	✓
DSA2	Your organisation would select a secure by design technology if it marginally (e.g. <10%) increased the unit cost per device.		✓	✓	✓	✓	✓
DSA3	Your organisation would select a secure by design technology if it significantly (e.g. >10%) increased the unit cost per device.		✓	✓	✓	✓	✓
DSA4	Your organisation would select a secure by design technology if it would reduce security vulnerabilities.		✓	✓	✓	✓	✓
DSA6	What are the key factors that your organization would need to consider if adopting a Digital Security by Design technology solution?		✓	✓	✓	✓	✓
DSA7	What obstacles would you face if migrating from your current technology to secure by design devices?		✓	✓	✓	✓	✓
DSA8	Are you aware of the National Cyber Security Centre's *Secure by Default* principles?	Y	✓			✓	✓
DSA9	*If Yes to above* Do you follow them in the development of your own product(s)?	Y	✓			✓	✓
DSA10	*If No to DSA8 or Partially to DSA9* What would your organisation need in order to better support the development of products that are secure by design?	Y	✓			✓	✓