Rapid Cybersecurity Assessment System for Small Business' COVID Move to Online

Tracy Tam
RMIT University
tracy.tam@student.rmit.edu.au

Asha Rao
RMIT University
asha.rao@rmit.edu.au

Joanne Hall
RMIT University
joanne.hall@rmit.edu.au

***Abstract*—COVID19 has made small businesses around the world rapidly adopt new online sales channels and tools. In this digital push for survival, the cybersecurity of the new systems has likely been forgotten. An existing global cybersecurity skills shortage means traditional individualised security assessments for these newly digital businesses are not practical. This paper proposes a web based self-assessment system (SE-CAP) to enable small business owners to conduct their own cybersecurity assessments. Designed with rapid deployability in mind, SE-CAP uses proven web based technologies to deliver a new solution to help small businesses become cyber-safe. The design of SE-CAP takes into account small business issues around record keeping, time constraints and poor technical literacy. The generic nature of the system allows SE-CAP's host organisation to customise and extend the self-assessment system beyond its initial scope. Challenges with industry cybersecurity knowledge gaps prevent SE-CAP's completeness. However, these gaps could be filled, in the interim, by the host organisation.**

I. Introduction

COVID19 has dramatically impacted the social fabric of society. It took away the traditional foot traffic, relied on by small businesses (0-19 employees [5]), by requiring social distancing and lockdown of our communities. Small businesses have had to, with little prior experience, quickly move online, or expand their online business to survive [26], [21]. As per the Australian Bureau of Statistics, in 2018, less than 40% of Australian small businesses derived more than half of their income from online sales [7].

Cybersecurity may have been missed in this rush to an online presence. Each new online storefront introduces a new suite of attack possibilities, as is evident from news reports of criminals taking advantage of opportunities and targeting new vulnerabilities as they emerge [12].

Compounding this challenge is the global cybersecurity skills shortage [4], [1]. There are currently insufficient cybersecurity professionals to conduct traditional one-on-one security audits for these newly digitised small businesses. An alternative approach is needed to protect small businesses.

Small business accounts for a significant portion of private-sector employment (in Australia, >40% [16]) and new job creation [30]. With employment fast becoming a key aspect of post-COVID recovery, the protection of small businesses is paramount. This will, in addition, protect the privacy and identity of the small business' customers, preventing serious personal, financial and emotional impacts [3].

Finally, very few small businesses have qualified IT support in-house [7]. (This trend is echoed with only a small portion of small businesses conducting security tasks in-house [18], or have an in-house qualified IT security expert [17].) With only a small proportion of small business engaged in a technical business venture [35], [6], the majority will need extra assistance with cybersecurity.

To address this urgent need to secure small businesses, we propose a Small Enterprise Cybersecurity Assessment Platform (SE-CAP). SE-CAP is a technology agnostic, rapidly deployable, online self-assessment system that will help small business owners protect themselves. SE-CAP's assessment process targets small business owners without a cybersecurity resource or the technical knowledge in-house to conduct a cybersecurity assessment, providing cybersecurity triage until the cybersecurity industry and official bodies fill the gap long term.

II. A Solution for An Unprecedented Time

SE-CAP is a self-assessment website intended to help small business owners create an IT asset inventory and to encourage incremental actions to mitigate basic cybersecurity vulnerabilities. The usage context and assessment logics to achieve this aim are illustrated in Figure 1 and Figure 2 respectively.

A. System Use

Primary user interactions with, and data inputs to, the self-assessment system are shown in Figure 1. The owners, through a browser, visit the SE-CAP URL. The small business owner inputs the existing IT device status of the business into the guided webpages. SE-CAP then matches that device and its configuration, with the applicable security controls. The small business is then linked to step by step instructions on how to implement the relevant security controls.

When the business owner implements the suggested controls, the control completion status is noted. At the end of the session, SE-CAP outputs a cybersecurity control status and inventory report for the small business owner to keep. Whenever their IT landscape changes, the business owner can

Workshop on Secure IT Technologies against COVID-19 (CoronaDef) 2021
21 February 2021, Virtual
ISBN 1-891562-72-X
https://dx.doi.org/10.14722/coronadef.2021.23004
www.ndss-symposium.org

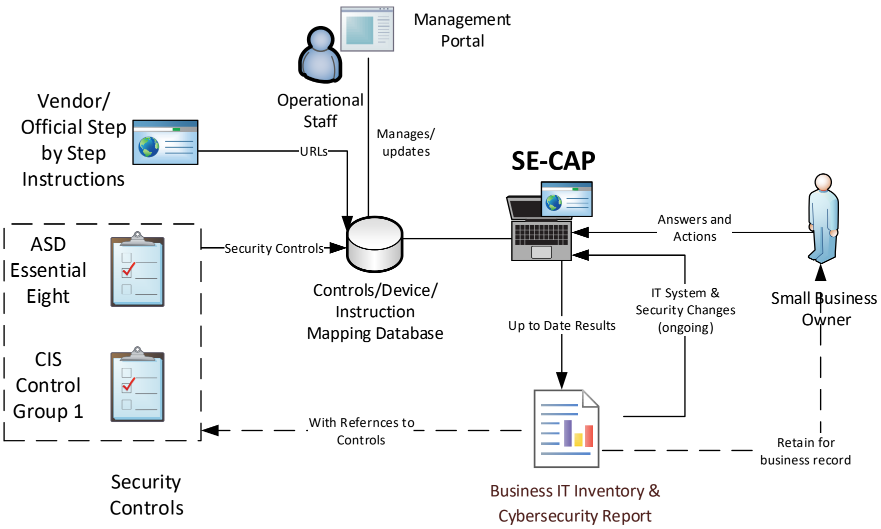

Management Portal
Operational Staff
Vendor/ Official Step by Step Instructions
URLs
Manages/ updates
SE-CAP
Answers and Actions
Small Business Owner
ASD Essential Eight
CIS Control Group 1
Security Controls
Controls/Device/ Instruction Mapping Database
Up to Date Results
IT System & Security Changes (ongoing)
With Refernces to Controls
Retain for business record
Business IT Inventory & Cybersecurity Report
Security Controls

Fig. 1. SE-CAP User and Data Interactions Model. Business owners interact with the SE-CAP via the publicly available website, ingesting and exporting human readable text files. This interaction is repeated if the user needs to update a new inventory detail. At the backend, SE-CAP is supported by a database which contains the mapping between security controls, devices and instructions to secure devices. User and data interaction steps are described in section II-A.

re-visit SE-CAP, load the old report into the webpage and generate a new report by changing their answers.

Supporting the SE-CAP webpage content is an internal database. This database is populated with current mappings between device relationship and cybersecurity controls, and between cybersecurity controls and official instructions on how to execute the controls. An operator is also responsible for maintenance of the mappings via a management portal, allowing for out-of-date mappings to be updated.

B. Small Business Design Factors

The design of SE-CAP is based on the key small business factors given below:

- Webpage as delivery mechanism: The choice of a well-known technology pattern, a website, makes SE-CAP:
  - deployable by any host organisation with an interest in small business cybersecurity, including non-technical official bodies.
  - reachable by any small business owner who has access to a web browser.
- Target Audience: Non-technical small business owners. The majority of small business owners have no technical background or are unfamiliar with technology [7], [31].
- Target Devices: Common consumer-grade devices, rather than enterprise grade products. Many micro and small businesses use consumer-grade IT products and/or share private devices with their business [9], [2].
- Reuse Before New Advice: The default approach is to re-use any official industry step by step instructions if available. This strategy avoids out of date advice and the overhead of a host organisation maintaining a separate set of instructions.

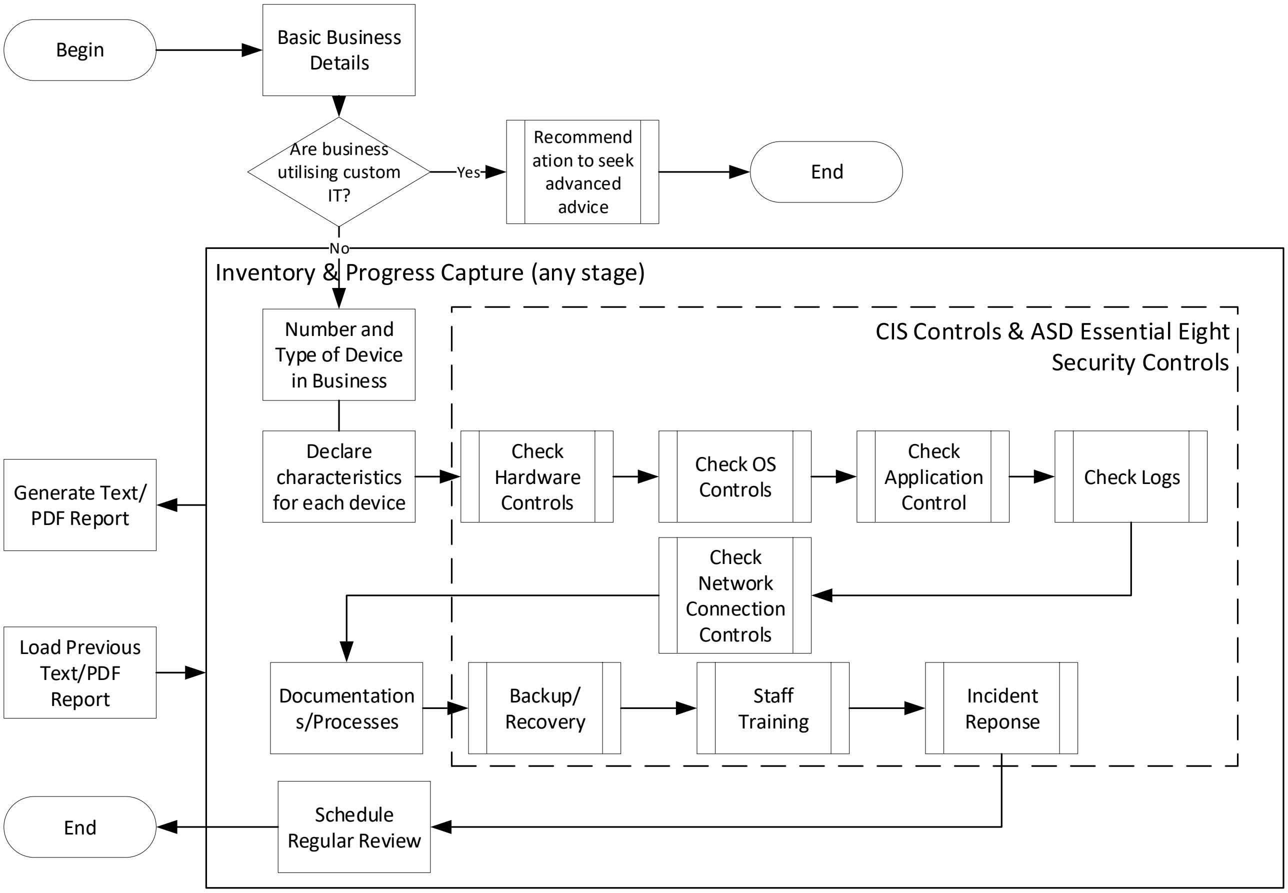
C. How Will the Self-Assessment Work?

Central to SE-CAP is a set of questions that guides small business owners through the process of securing each asset. The logic of the assessment that the user sees is illustrated in Figure 2, and described below.

1) Vetting Users: Before starting, the SE-CAP website asks the small business owner (the user) simple questions around the business size and IT complexity. If the user is shown to require more sophisticated assistance beyond consumer-grade computer devices, i.e. beyond SE-CAP scope, they are advised to contact cybersecurity professionals.

Once the business is found to be in scope, SE-CAP prompts the user to take stock of the number and types of business devices, network connections and processes. The SE-CAP then delves deeper by asking questions around hardware, operating system and applications. Based on the device characteristics, the internal database will dynamically generate a list of cybersecurity actions that are relevant. The cybersecurity control recommendations are based on existing cybersecurity industry standards; further discussion is in Section II-E.

2) Individual Devices - One at a Time: Each list of cybersecurity control actions is tied to a specific business device/process. For example, a device should have updates applied regularly. If the user states a computer is running on Windows, they are reminded to turn on automatic updates OR schedule a regular task each week to perform the update for that device. Instructions on how to perform the actions are linked to external official instruction sites. In this example, the instruction will link to Microsoft's official help site on



Begin
Basic Business Details
Are business utilising custom IT?
Yes
Recommend ation to seek advanced advice
End
No
Inventory & Progress Capture (any stage)
Number and Type of Device in Business
Declare characteristics for each device
CIS Controls & ASD Essential Eight Security Controls
Check Hardware Controls
Check OS Controls
Check Application Control
Check Logs
Check Network Connection Controls
Generate Text/ PDF Report
Load Previous Text/PDF Report
Documentation s/Processes
Backup/ Recovery
Staff Training
Incident Reponse
Schedule Regular Review
End

Fig. 2. Logic Flow of SE-CAP Questions for End Users: SE-CAP will first vet users for their suitability to use SE-CAP. Then SE-CAP collects information for the IT devices inventory. Collected device characteristics are used to display relevant instructions that helps users meet security controls from ASD Essential Eights and CIS Controls. The result of the process can be updated, paused and resumed via user save text/pdf reports. For detail description, see Section II-C

how to turn on automatic updates and/or apply updates manually. If the business operates a second Windows device, the information will be presented again for the second device. The repetition of advice for each device provides step by step clarity and focus for end users, and prevents logic jumps that may leave devices un-actioned.

3) Keeping Track: As the user completes each action, they are invited to note it in SE-CAP. They are given the options to skip actions at any time, e.g. enabling multi-factor authentication (MFA), for usability. Skipping allows scenarios where the device/action can't be completed immediately (e.g. a business is waiting for a software vendor's instructions on how to enable MFA). The lack of action will be noted in the output, and users will be reminded of the action(s) still to be completed when the process is resumed.

The relevant industry standard controls completed are noted in the output file, as the user goes through each section. This tracking facilitates a traceability of the effort that the business owner has invested into the process, thus providing a clear feedback loop [24] showing that their actions do have an impact on their vulnerability profile.

4) Pause Anytime: Users can pause and save via a local file export in a human-readable file, e.g. text, pdf etc, at any stage. When they are ready to resume the process, the same file is re-ingested into the website for editing. This record serves 2 main purposes:

- A saved file that a user can resume at a later stage.
- A business' IT inventory record and the cybersecurity state at a point in time. Both of these provide valuable information in future cybersecurity activities for internal and external stakeholders e.g. cybersecurity professionals.

This import/export function also allows business owners to easily update their existing inventory and security controls list.

5) A Continuous Process: Ideally, small business owners will complete SE-CAP in short sessions over multiple weeks. There are no limitations on the number of times and the length of time small business owners should spend on SE-CAP each time, allowing for flexibilities. For example, John, a small business owner, has a small window of time each Monday morning as he waits for a meeting to begin. John spends 15 minutes on SE-CAP and saves and resumes his progress over many weekly 15 minute sessions. Jane, on the other hand, suddenly had a 2 day training course cancelled. Jane can work through SE-CAP during those 2 days, exporting and resuming at the end of each day. In this case, SE-CAP would encourage Jane to schedule time slots in her calendar to revisit her answers.

The potential benefit of a repeated interaction model between SE-CAP and the user is the creation of an ongoing relationship and awareness of cybersecurity inside their business.

D. The Benefits of Self Assessment

SE-CAP's self-assessment model takes the opposite approach to the current cybersecurity industry model of individualised assessment. Self-assessment is a model that government and industry bodies have used to provide advice for other aspects of running a business e.g. licensing [11], food labeling [20] etc. A self-help approach is a valid strategy for small businesses, with the Australian Business Licensing Information Service (ABLIS) [11] (which connects business owners to disparate existing local licensing requirements and bodies) recording over 200,000 searches in the 2018-19 financial year [10].

SE-CAP's self-assessment deliberately places the tools within the hands of the business owner rather than the cybersecurity professional. The 2 main drivers for the self-assessment recommendations are:

- The reality that a cybersecurity professional is out of reach for small businesses, financially and logistically.
- The creation of a sense of self-efficacy and ownership of the security of their IT systems amongst small business owners.

The drive to raise self-efficacy is founded on established Protection Motivation Theory (PMT) research [27]; humans are more likely to take action to protect themselves if they feel that actions they take can lead to an effective outcome. Public health campaigns have successfully used PMT theories to promote individual actions for self protection [19] and information security is now starting to do the same [37], [25].

In SE-CAP, we promote self-efficacy by formulating questions based on IT concepts (i.e. devices) that small business owners are familiar with, thus clarifying the control that the small business has. The process further de-mystifies cybersecurity measures by linking the controls to tangible devices, thus increasing a sense of control and familiarity [27]. Encouraging protective behaviours encourages good cybersecurity habits from the small business owner themselves.

SE-CAP works well in a "working from home" scenario, as necessitated by COVID-19 restrictions in some countires. Work from home introduces the complexity of a delicate balance between privacy and thoroughness that many businesses of various sizes are working through.

By asking each employee to perform SE-CAP individually and reporting back on their level of compliance gives business owners the assurance that a certain level of security has been followed, while leaving the details of the employee's home IT setup relatively private.

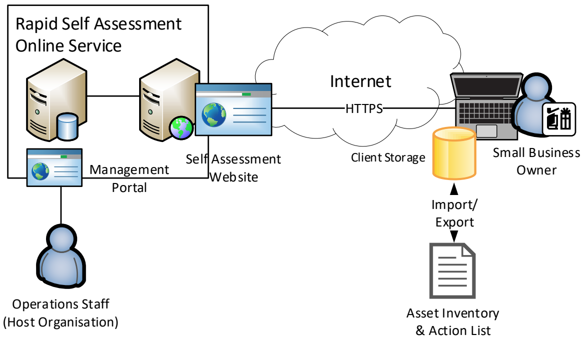


Fig. 3. Self Assessment System Reference Architecture: SE-CAP reference architecture contains only a handful of generic components. The main architecture blocks include web application, database, URL, internet and an internet enabled user device. These architecture blocks can be implemented using a variety of widely available technologies. See Section III for further details.

E. The Security Controls

The questions, the actions, and how these are presented hold the key to the usability of SE-CAP. To this end, the questionnaire in SE-CAP centers on language and objects that users are familiar with: device, Internet connection and business processes. The value of SE-CAP is in relating everyday business concepts back to established cybersecurity standards in a meaningful and measurable way.

The questions and control actions are initially based on two established cybersecurity standards: CIS Control [13] and the Australian Signal Directorate's (ASD) Essential Eight [8]. These standards are chosen for:

- Device centric approach,
- Incremental process starting from small actions,
- Traceability and clear migration path into a comprehensive security standard.

A clear migration path to a comprehensive standard is critical to a business' journey, as cybersecurity readiness is a continuous process. These 2 standards provide a path, when the need arises, to further develop a small business' security posture.

CIS Control and ASD Essential Eight's control points are separated into device, network connections and process categories for SE-CAP. In SE-CAP the control points do not follow the sequence given in either standard, as neither standard claims any strict order dependency. When the output document is exported, the user is shown a list of control points that have been fulfilled and not fulfilled from each standard.

III. System Architecture

SE-CAP intentionally uses generic web technologies to increase a host organisation's ability to deploy and maintain. SE-CAP's reference architecture as described in Figure 3.

SE-CAP can be developed in any programming language that supports client-side data, server-side database, web-forms and basic logic. At a high level, SE-CAP is a web application attached to a database. This web application is made available, via web front-end servers, to the Internet. End user access is via an advertised URL (over HTTPs for secure data carriage).

Generic assessment information is served from the server to the client to enable the display of pages. The bulk of the business specific data, i.e. what the user inputs, are confined to the client-side for security purposes.

Note that the precise technology to employ will depend on the technology stack and capability of the host organisation. All mentions of specific technologies are merely an example, and the best option must be chosen to suit the target hosting environments.

A. *Client Side Technology*

One noted architectural difference between SE-CAP and a common website is the heavy reliance on client-side storage. The client data storage serves as additional privacy protection, in addition to the HTTPs connectivity, to minimise transit of sensitive business data over unsecured networks. This also minimises the sensitive data to be stored and dealt with by the server. All persistent data is stored on the client-side only, see Figure 4. The persistent client data gets exported as a local file that the small business owner retains.

The client-side storage of data, using technology such as IndexedDB [36], Cache Storage API [28] etc, prevents transmission of sensitive data across potentially untrusted network connections. The information sent from server to client is at a high level and does not include precise details of business specific devices/processes.

The implementation of a client-side heavy design is an unconventional architectural decision, which has associated challenges that will be discussed in Section IV-A.

B. *Inventory/Progress File*

The data saving mechanism as an output of the self-assessment is intended to be a record for the small business. This is provided in the form of client-side text file export libraries e.g. jsPDF [29]. The client-side libraries are recommended to address the data storage and security risks associated. At no stage are the servers expected to process or save the data that business owners input.

Regardless of implementation technology, the import/export files must:

- Be human readable, serving both as a saved file and a business record,
- Contain progress of questions, actions and references completed and outstanding,
- Contain referenced security controls that have been marked as completed.

By serving multiple purposes, SE-CAP allows for easier maintenance and a smaller footprint.

C. *Management Portal*

Another important aspect of SE-CAP is the management interface of the database. This allows the database to be updated with changes to any aspects of the security controls and associated data. The changes will then allow the latest external references to be presented to small business owners, ensuring ongoing relevance of the advice. The rapidly changing nature of IT and cybersecurity means that a dedicated management portal on SE-CAP for the operational staff to change this information is required. Requiring code update on the website to change minor details such as links is not practicable for the long term viability of SE-CAP.

D. *Real (or Near Real) Time Support*

To further increase the self-efficacy of the user, optional live support functions can be deployed using many existing technologies, ranging from live chats, peer support forums to ticket based systems. While not a core function, the ability to assist users would be beneficial in both helping users and being able to receive feedback on how SE-CAP can be improved. Existing psychological theory [33] points to the role that supportive relationships can play in changing behaviour. For many business owners, especially non-technical users who may be undertaking cyber-security audits for the first time, this support can provide the encouragement to persist with this exerecise.

The choice of technology used to provide support to users will depend upon existing norm and conventions, within the host organisation.

IV. Challenges of Self-Assessment System

Despite technical flexibility and reuse of proven web technology, there are challenges to implementing SE-CAP. Some of these can be solved by an investment in architectural design and integration efforts. There are also several non-technical considerations that need further investigation.

A. *Client Emphasis*

Due to the unusual architecture of relying heavily on client-side web browser execution in both logic and data of SE-CAP, some features of server-side processing are not available. When deploying this solution, host organisations must consider the following aspects:

- Performance - The use of client-side logic places significant processing workload on the client-side browser. Depending on the expected computing power that the small business users are likely to have, a re-balancing between the amount of client-side processing and confidentiality of data may be required. It may be necessary to place certain business sensitive data back onto the server-side to alleviate client computing load.
- Data Validation - An advantage of server-side storage of data is the ability of the server to validate data passed in by a client. As server-side data validation is not possible in this solution, developers of the platform need to be mindful of the increased likelihood of faulty inputs from the client side and develop the system to handle and secure against these scenarios.

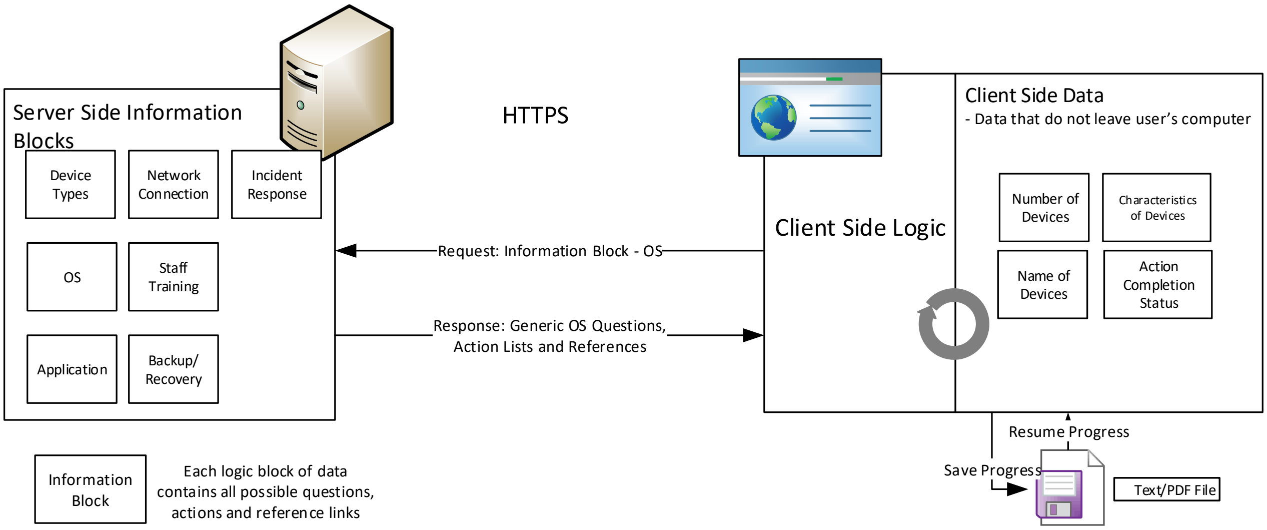

Server Side Information Blocks
Device Types
Network Connection
Incident Response
OS
Staff Training
Application
Backup/ Recovery
HTTPS
Request: Information Block - OS
Response: Generic OS Questions, Action Lists and References
Client Side Logic
Client Side Data
- Data that do not leave user's computer
Number of Devices
Characteristics of Devices
Name of Devices
Action Completion Status
Resume Progress
Save Progress
Text/PDF File
Information Block
Each logic block of data contains all possible questions, actions and reference links

Fig. 4. High Level Server vs Client Data Storage and Data Interactions at a Software Level: The sensitive business data, in the ideal architecture, never leaves the client machine. Blocks of generic question are sent from the server, and processed on the client side for display. See Section 4 for further details.

B. Usability for Small Business Owners

The ability to use SE-CAP largely depends on small business owners being able to understand and answer the questions on their own. To enable this, all user related aspects of the system must be carefully crafted in language and functions familiar to a non-technical audience. While it is expedient to use the language within each relevant cybersecurity standard, this language is not understood by all business owners [9]. As an example, to address CIS Control 1.6 [13], SE-CAP can ask questions around whether there are any strange computers or phones in their router list of connections, rather than framing questions in terms of "unauthorised assets" as described in the control. At a terminology level, usability can also be enhanced by using specific terms such as "phone", "internet router", "laptop" etc. in place of an industry (but technically correct) term such as "device". A non-technical user is not likely to understand the underlying assumption that "device" encompass a variety of types of equipment.

The legibility of the language used is vitally important, as the primary audience of SE-CAP is unlikely to have the technical training or experience that cyber-security professionals have. At a practical level, one way of supporting the empowerment of small business owners is to conduct user experience design activities to ensure the appropriateness of the language used.

C. Gaps Between & In Cybersecurity Standards

Most cybersecurity standards do not cover all aspects of cybersecurity practices at a day to day level. One notable gap is around incident response: the actions required to be taken once a breach has occurred. Most advice has centred around prevention. Post-breach help in varied degrees that has been set up by governments worldwide [22], [23], mostly targets private individuals. Current advice is far from useful for small businesses, despite a small business' intertwined relationship with their owners. Our analysis for this solution proposal has identified a significant lack of official small business cybersecurity incident response measures.

Incident response advice needs to be included as part of SE-CAP. In the interim, the host organisation of SE-CAP, with a specific audience in mind, will be best placed to put together that advice. This custom advice is a short term remediation until a long term industry approach is developed.

Other gaps may be discovered within the standards during detailed security control and question mapping activities. Knowledge gaps will need to be filled by SE-CAP's host organisation on a case by case basis until a coordinated industry approach is found.

D. Legal Considerations

Due to the advisory nature of SE-CAP, its legal status will change depending upon SE-CAP's host entity. A few points which should be considered, from the host organisation's perspective are:

- Regulatory framework for business advice,
- Existing local laws around cyber crimes,
- Existing local processes and support around cyber crimes/identity theft,
- Host's relationship with the small business owner,
- Any specific industry regulations.

E. Host Organisation

In recent years, cyber-security has been debated in many contexts [34], [15] as a public good. Countries like Singapore now treat the cyber-security of its community similar to basics such as sanitation and product safety [14]. Cyber-security can no longer be considered a purely private good from an economic point of view. The support of small business cyber-security protects not just the small business owners, but also the data and identities of their customers and any associated entities.

As a tool that enables the delivery of a collective cyber-security good, it is imperative to recognise that there are multiple candidate host organisation(s) suitable for the hosting of SE-CAP, e.g. government deparments, industry associations or statutory bodies. Other than a host that can supply the technical resource and management requirements already discussed thus far, considerations from the perpective of best arranagement to provide cyber-security as a common/public service needs to be further studied. It is a topic that can greatly benefit from the learnings and lessons from the field of collective good/services policies [32].

V. Extendibility

SE-CAP can be expanded with the inclusion of further cybersecurity standards and specialisations. A particular industry may choose to add industry-specific questions and controls upon this base. By starting with the universal building blocks of cybersecurity in the users and IT devices, the data and question model can be extended to suit niche or specialised situations.

VI. Conclusion

We have proposed SE-CAP to deal with the current surge in small business online activities due to COVID19. A distributed and self-help system has the best chance of reaching a large audience due to the current lack of cybersecurity expertise and resources. By making cybersecurity approachable and achievable for even the least technical of business owners, SE-CAP has the potential to lift the cybersecurity posture of the small business cohort. The incremental improvement in security posture will benefit both small businesses and the cybersecurity industry, by limiting the number of “easy” targets that criminals can exploit. The limiting of the number of targets will eventually allow more focused investigation by law enforcement, and as a result better legal remediation potential for victims.

Acknowledgment

This research is supported by an Australian Government Research Training Program (RTP) Scholarship.

References

[1] R. J. Ackerman, “The Cyber Skills Shortage Continues to Balloon – and Think Tanks Aren’t Helping,” 2019. [Online]. Available: https://www.rsaconference.com/industry-topics/blog/the-cyber-skills-shortage-continues-to-balloon-and-think-tanks-arent-helping

[2] D. Almubayedh, M. A. Khalis, G. Alazman, M. Alabdali, R. Al-Refai, and N. Nagy, “Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study,” *21st Saudi Comput. Soc. Natl. Comput. Conf. NCC 2018*, pp. 1–6, 2018.

[3] D. Armstrong, “I Lost My Identity to a Fraudster, and It Took Six Years to Clean Up the Mess,” Aug. 2019. [Online]. Available: https://www.bloomberg.com/news/articles/2019-08-12/i-lost-my-identity-to-a-fraudster-and-it-took-six-years-to-clean-up-the-mess

[4] AustCyber, “Australia’s Cyber Security Sector Competitiveness Plan 2019 Update,” 2019. [Online]. Available: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019

[5] Australian Bureau of Statistics, “1321.0 - Small Business in Australia, 2001,” 2001. [Online]. Available: https://www.abs.gov.au/ausstats/abs@.nsf/mf/1321.0

[6] ——, “8165.0 - Counts of Australian Businesses, including Entries and Exits, June 2014 to June 2018,” 2019. [Online]. Available: https://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0June2014toJune2018?OpenDocument

[7] ——, “8167 Selected Characteristics of Australian Business,” 2019. [Online]. Available: https://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/C575766838376FA0CA2573E1000E3F2F?opendocument

[8] Australian Cyber Security Centre, “Australian Signal Directorate Essential Eight Maturity Model,” pp. 1–2, 2019. [Online]. Available: https://www.cyber.gov.au/node/100https://www.cyber.gov.au/publications/essential-eight-explained

[9] ——, “Supporting Small Businesses – The ACSC Small Business Cyber Security Guide and Companion Materials,” Australian Cyber Security Centre, Tech. Rep., 2019.

[10] Australian Government, “ABLIS Analytics Dashboard,” 2020. [Online]. Available: https://ablis.business.gov.au/reports

[11] ——, “Australian Business Licence and Information Service,” 2020. [Online]. Available: https://ablis.business.gov.au/

[12] Australian Signals Directorate- Government of Australia, “Threat Update: COVID-19 malicious cyber activity,” Australian Cyber Security Centre, Tech. Rep., 2020. [Online]. Available: https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020

[13] Center for Internet Security, “CIS Controls,” Center for Internet Security, Tech. Rep., 2019. [Online]. Available: www.cisecurity.org/controls/

[14] Cyber Security Agency of Singapore, “Our Organisation,” 2020. [Online]. Available: https://www.csa.gov.sg/who-we-are/our-organisation

[15] Danilo D’Elia, “The Economics of Cybersecurity: From the Public Good to the Revenge of the Industry,” in *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2016, vol. 9588, pp. 3–15.

[16] Department of Parliamentary Services, “Small business sector contribution to the Australian economy,” 2018. [Online]. Available: https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/6272043/upload_binary/6272043.pdf

[17] V. Dimopoulos, S. Furnell, M. Jennex, and I. Kritharas, “Approaches to IT Security in Small and Medium Enterprises,” in *Proc. 2nd Aust. Inf. Secur. Manag. Conf. Secur. Futur. Perth, West. Aust. Novemb. 26th, 2004*, 2004, pp. 73–82. [Online]. Available: https://www.researchgate.net/publication/221148270_Approaches_to_IT_Security_in_Small_and_Medium_Enterprises

[18] Eurostat, “ICT security in enterprises,” 2020. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/pdfscache/9132.pdf

[19] D. L. Floyd, S. Prentice-Dunn, and R. w. Rogers, “A Meta-Analysis of Research on Protection Motivation Theory,” *J. Appl. Soc. Psychol.*, vol. 30, no. 2, pp. 407–429, 2000.

[20] Food Standards Australia New Zealand, “Nutrition Panel Calculator,” 2019. [Online]. Available: https://www.foodstandards.gov.au/industry/npc/Pages/Nutrition-Panel-Calculator-introduction.aspx

[21] N. Gallagher, “One of KC’s best craft cocktail bars adapts with bottled drinks and kits during coronavirus quarantine,” *Kansas City Mag.*, Mar. 2020. [Online]. Available: https://www.kansascitymag.com/cocktail-hour-during-coronavirus-outbreak/

[22] IDCare, “IDCare,” 2019. [Online]. Available: https://www.idcare.org

[23] JND Legal Administration, “Equifax Data Breach Settlement,” 2020. [Online]. Available: https://www.equifaxbreachsettlement.com/en/amend

[24] K. A. Karl, A. M. O’Leary-Kelly, and J. J. Martocchio, “The Impact of Feedback and Self-Efficacy on Performance in Training,” *J. Organ. Behav.*, vol. 14, no. 4, pp. 379–394, 1993.

[25] Y. Li, J. Wang, and H. R. Rao, "Adoption of identity protection service: An integrated protection motivation – precaution adoption process model," *AMCIS 2017 - Am. Conf. Inf. Syst. A Tradit. Innov.*, vol. 2017-Augus, pp. 1–9, 2017.

[26] J. Longbottom, "Coronavirus forces businesses to adapt to survive the COVID-19 pandemic," *ABC News*, Mar. 2020. [Online]. Available: https://www.abc.net.au/news/2020-03-19/how-businesses-adapting-to-survive-covid-19-coronavirus/12068696

[27] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983.

[28] Mozilla Developer Network, "CacheStorage," 2020. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/API/CacheStorage

[29] MrRio, "jsPDF Library," 2020. [Online]. Available: https://github.com/MrRio/jsPDF

[30] Organisation for Economic Co-operation and Development (OECD), "Productivity by industry," *Oecd Product. Indic. Compend.*, 2018.

[31] ——, "Survey of Adult Skills (PIAAC): Full selection of indicators," Paris, 2019. [Online]. Available: https://gpseducation.oecd.org/IndicatorExplorerhttps://doi-org.ezproxy.lib.rmit.edu.au/10.1787/eco_surveys-aus-2018-graph60-en.

[32] V. Ostrom and E. Ostrom, "Public Goods and Public Choices," in *Polycentricity Local Public Econ. Readings from Work. Polit. Theory Policy Anal.* University of Michigan Press, 1999, p. 75.

[33] J. Prochaska, C. Diclemente, and J. Norcross, "In Search of How People Change: Applications to Addictive Behaviors," *Am. Psychol.*, vol. 47, no. 9, pp. 1102–1114, 1992.

[34] M. Taddeo, "Is Cybersecurity a Public Good?" *Minds Mach.*, vol. 29, no. 3, pp. 349–354, 2019. [Online]. Available: https://doi.org/10.1007/s11023-019-09507-5

[35] U.S. Small Business Administration, "2019 Small Business Profile," U.S. Small Business Administration, Office of Advocacy, Tech. Rep., 2019. [Online]. Available: https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142719/2019-Small-Business-Profiles-US.pdf

[36] W3C, "Indexed Database API 2.0," 2018. [Online]. Available: https://www.w3.org/TR/IndexedDB-2/

[37] I. M. Woon, G. W. Tan, and R. T. Low, "A protection motivation theory approach to home wireless security," *Assoc. Inf. Syst. - 26th Int. Conf. Inf. Syst. ICIS 2005 Forever New Front.*, pp. 367–380, 2005.