IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 June 2022, accepted 26 June 2022, date of publication 29 June 2022, date of current version 12 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3187211

RESEARCH ARTICLE

How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond

NAN SUN[1,2], CHANG-TSUN LI[3], (Senior Member, IEEE), HIN CHAN[4], MD ZAHIDUL ISLAM[5], MD RAFIQUL ISLAM[6], (Senior Member, IEEE), AND WARREN ARMSTRONG[7]

[1]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2612, Australia
[2]Cyber Security Cooperative Research Centre, Joondalup, WA 6027, Australia
[3]School of Information Technology, Deakin University, Waurn Ponds, VIC 3216, Australia
[4]Australian Cyber Security Centre, Kingston, ACT 2604, Australia
[5]School of Computing, Mathematics and Engineering, Charles Sturt University, Bathurst, NSW 2795, Australia
[6]School of Computing, Mathematics and Engineering, Charles Sturt University, Albury, NSW 2640, Australia
[7]QuintessenceLabs Pty Ltd., Canberra, ACT 2609, Australia

Corresponding author: Nan Sun (nan.sun@adfa.edu.au)

This work was supported in part by the Cyber Security Research Centre Ltd., through the Australian Government's Cooperative Research Centers Program.

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by Deakin University and Charles Sturt University Human Research Ethics Offices with the Reference Number SEBE-2021-38 and Protocol Number H21353, respectively, and performed in line with the National Statement on Ethical Conduct in Human Research 2007 (Updated 2018).

ABSTRACT Cyber assurance, which is the ability to operate under the onslaught of cyber attacks and other unexpected events, is essential for organizations facing inundating security threats on a daily basis. Organizations usually employ multiple strategies to conduct risk management to achieve cyber assurance. Utilizing cybersecurity standards and certifications can provide guidance for vendors to design and manufacture secure Information and Communication Technology (ICT) products as well as provide a level of assurance of the security functionality of the products for consumers. Hence, employing security standards and certifications is an effective strategy for risk management and cyber assurance. In this work, we begin with investigating the adoption of cybersecurity standards and certifications by surveying 258 participants from organizations across various countries and sectors. Specifically, we identify adoption barriers of the Common Criteria through the designed questionnaire. Taking into account the seven identified adoption barriers, we show the recommendations for promoting cybersecurity standards and certifications. Moreover, beyond cybersecurity standards and certifications, we shed light on other risk management strategies devised by our participants, which provides directions on cybersecurity approaches for enhancing cyber assurance in organizations.

INDEX TERMS Common criteria, cyber security, protection profile, security standard and certification, trusted system.

I. INTRODUCTION

According to the statistics from Dell Technology in 2019/2020, 44% of organizations have experienced at least one cybersecurity attack or data breach during the prior twelve months [1]. Security issues are becoming a daily struggle for public and private sectors alike. Data from the Australian Cyber Security Centre's (ACSC) Annual Cyber Threat Report [2] shows that the number of cybersecurity attacks is still on the rise. As the consequences of a cybersecurity attack, an organization's financial and reputational health may be affected, business operations are disrupted, sensitive information including intellectual property may be stolen, and malicious activity may continue [3].

Although it is difficult to quantify the costs of impacts, cybersecurity remediation can be more expensive than early

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

and ongoing investment in prevention [4]. To reduce the potential impact of cyber attacks, risk management that involves the process of identifying, assessing, and taking steps to minimize security risks is essential as a cybersecurity approach for organizations. Having cybersecurity awareness and robust security strategies in place can help organizations prepare for, protect against, and respond to cyber attacks to some extent [5]. Since Information and Communication Technology (ICT) products are widely used by organizations and individual users, choosing trusted ICT products is of paramount importance for the organization's risk management. The existing cybersecurity standards and certifications for evaluating ICT products provide guidelines for vendors to design, develop, evaluate, certify their products, as well as provide trusted references for users to choose the products.

The Common Criteria for Information Technology Security Evaluation (often referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408), which certifies that systems and products to ensure they meet predefined security requirements [6]. The Common Criteria covers comprehensive ICT security-related technologies and a wider range of evaluation aspects regarding security functionalities and security assurance [7]. Security requirements for a class of related products are typically predefined in a Protection Profile by a user group or user [6]. The purpose of a Protection Profile is to provide reusable templates of security requirements to support the definition of functional security standards and guide the formulation of product development and procurement specifications.

Generally, the subject of the evaluation that can be part of the product or system is called the Target of Evaluation. A Security Target is a document that identifies the security features of the Target of Evaluation [8]. If a vendor has an ICT product that they would like to be evaluated and certified under the Common Criteria, they must complete a Security Target description. The vendor should conduct a self-assessment on compliance with the Protection Profile prior to evaluation against the profile. Evaluation are conducted in laboratories to validate the product's security features and confirm that it meets the security requirements outlined in the Security Target [9]. Following the evaluation of ICT products and systems via a set of specifications and guidelines, the products that passed the evaluation are awarded the Common Criteria certification [10] and be listed on the Common Criteria portal [11].

The Common Criteria certification assures consumers that the products they invest in provide reliable security protection for their operational environment and conform to the vendor's claims. Furthermore, the Common Criteria certification increases the competitiveness of vendors' products when consumers compare them to similar products on the market. For government agencies, the Common Criteria certification not only facilitates procurement but increases the transparency of ICT products' security features, facilitating market supervision and surveillance. However, there is a lack of widespread adoption of evaluated ICT products with security functionality by organizations, including governments and commercial sectors [12]. For instance, although Australia is a signatory to the Common Criteria Recognition Arrangement (CCRA), the number of certifications through the Australian Information Security Evaluation Program is trivial when compared to the number of certificated products on Common Criteria's Certified Products List [13].

In this paper, we aim to identify the adoption barriers for security standards and certifications, especially the one which covers the most extensive category of ICT products, the Common Criteria. Through 258 responses to an online questionnaire from participants from Australian and international organizations, we analyze the organizations' attitudes towards being measured against cybersecurity standards and their adoption of the cybersecurity standards. Our participants also describe risk management strategies, such as reactive and proactive cybersecurity countermeasures and multi-layered risk management approaches, adopted by their organizations to pursue cyber assurance. To achieve our aim, in this paper, we address the following research questions:

RQ1: *What are the adoption barriers of the Common Criteria?*

RQ2: *How to promote the adoption of the Common Criteria?*

RQ3: *How do organizations seek cyber assurance beyond adopting security standards and certifications?*

To answer RQ1, based on the identified adoption barriers from the literature review, we design the questionnaire to investigate the adoption barriers for the Common Criteria in Section IV-A. Recommendations for promoting Common Criteria adoption as well as the other security standards and certifications are presented in Section IV-B towards answering RQ2. Beyond the security standards and certifications, the adopted approaches to cyber assurance are discussed in Section V to address RQ3.

II. RELATED WORK

A. CYBERSECURITY STANDARDS AND CERTIFICATIONS

The applications and adoption of cybersecurity standards and certifications for ICT products and systems have been explored and discussed in previous studies. As ICT products are designed, developed, and implemented, cybersecurity standards and certifications play a significant role, especially in areas such as the Internet of Things (IoT) [5], smart grids [14], and software [15]. The recent study [5] reviewed cybersecurity standards and certifications for the IoT ecosystem by analyzing the various standards and certifications schemes and the challenges associated with implementing them. Additionally, previous works [16]–[18] reviewed the key building blocks for the certification process in the context of security testing and risk assessment in IoT. Along with security certifications for IoT, Leszczyna *et al.* [14] conducted a study that examined smart grid cybersecurity standards and provided insights into the adoption of cybersecurity standards. Specifically, the work [14] examined

36 cybersecurity-related and 12 privacy-related standards and their adoptions in the area of smart grid. Additionally, Kara *et al.* [15] reviewed the Common Criteria in a specific field, which shed light on the Common Criteria's application in secure software development.

Since Common Criteria covers a comprehensive range of categories and technologies for ICT products and services, it promotes the mutual recognition of secure ICT products among a broad range of security standards and certifications [19]. For example, Matheu *et al.* [5] stated that Common Criteria is the most widely used cybersecurity certification in the IoT field. Furthermore, albeit the fact that Russia is neither a Certificate Authorizing Participant nor a Certificate Consuming Participant of the Common Criteria, the history, structure, and features of the Common Criteria used in the Russian scheme are reviewed in [20] and [21]. The Common Criteria standard has also been adopted worldwide by other non-Common Criteria Recognition Arrangement nations, such as China, which has its own certification scheme with their adaption of the Common Criteria standard called GB/T 18336 [22]. In spite of the significant role of the Common Criteria in ensuring cybersecurity through security standards and certifications, widespread adoption of the Common Criteria and certified products is still a long way off [12]. In this work, we investigate adoption barriers of security standards in the case of the Common Criteria by adopting the survey approach. Aside from the adoption barriers identified from the literature review being validated by our designed questionnaire, we explore other previously overlooked adoption barriers.

B. CYBER ASSURANCE AND RISK MANAGEMENT

Security risk management refers to the process of *"identifying, assessing, and taking steps to reduce security risks to an acceptable level"* according to the definition from the Australian Cyber Security Centre [23]. Additionally to cybersecurity standards and certifications, organizations employ a variety of risk management strategies, which include physical controls (e.g., alarm systems, biometrics, etc.), technological controls (e.g., firewalls, encryption, etc.), and behavioral controls (e.g., security training, policies and procedures, etc.). The topic of risk management for cybersecurity assurance in different industry sectors has been extensively researched from the perspective of technology [24]–[27], theoretical perspective [28], as well as the practice perspective [29]. For example, the study by Ghadge *et al.* [25] focused on cyber risk management in supply chain contexts by conducting a systematic literature review. A clear understanding of the cyber risk challenges and mitigation strategies helps supply chain managers make informed decisions. The paper by Ahmad *et al.* [29] provided an in-depth case study of a financial organization and outlined a process model that can be used to increase situation awareness in organizations.

Furthermore, numerous studies offer valuable insights into better risk management in organizations [30]–[33]. For instance, Hoppe *et al.* [26] gathered market insights from 37 recent industry surveys and structured them based on the steps of the risk management process. Through the study, the researchers [26] found that a lack of security experts and a strained market were the main obstacles to implementing cyber risk management for small and medium-sized businesses. From the strategic aspects of risk management, Laube *et al.* [32] systematically reviewed works on cyber risk information sharing, which is proved to be beneficial in providing more edges to the defenders in their races against cyber attackers. Tounsi and Rais [33] argued that the defenders are required to collect and understand cyber-threat intelligence to cope with the ever-increasing sophistication of cyber threat intelligence. To investigate the role of cyber insurance in risk management, Biener *et al.* [30] conducted an empirical analysis on the insurability of cyber risks. After assessing the market potential in light of the increasing number of high-profile cyber incidents, they concluded [30] with a positive note on cyber insurance.

Nevertheless, organizations in various industry verticals are still vulnerable to cyber risks and continue to suffer from damages, such as financial loss, data breach, and even reputation loss, caused by cyber attacks [3]. As part of our research, we investigate, through questionnaires, how organizations in different countries and industries currently seek cyber assurance and risk management in addition to cybersecurity standards and certifications. Combined with the practice, strategies and insights from the previous research work, we further provide the risk management best practices for cyber assurance at a high level.

III. OUR INVESTIGATIONS

To investigate how organizations seek cyber assurance and their adoption of security standards, especially the Common Criteria, we tried to find participants across different sectors, countries and organizations of various sizes. We collected responses to our questionnaire through Qualtrics from 22 Sep 2021 to 23 Dec 2021 to seek answers to the three research questions we raised in the Introduction. Our study received ethics approval from Deakin University and Charles Sturt University Human Research Ethics Office with the Reference Number SEBE-2021-38 and Protocol Number H21353, respectively. See survey at: https://github.com/nansunsun/DACCA_Questionnaire/blob/main/DACCA_Questionnaire.pdf. This section discusses the questionnaire design, data collection, and analysis of the responses.

A. QUESTIONNAIRE DESIGN AND DATA COLLECTION

There are 28 questions in the questionnaire, including open-ended and closed-ended questions in the forms of short answers or multiple-choice questions. We first investigated participants' demographics using Q1 - Q4 (Question 1 to Question 4), including the organization's name, countries where the participant's organization operates, the size of the organization, and the sectors wherein the participant's organization conducts its businesses.

TABLE 1. The number of each sector of participants' organizations belong to. One participant can choose more than one sector. The statistics are based on 158 participants who disclosed the sectors where their organizations operate in.

Sector name	Count
Defence industry	39
Health and social care	19
Food and agriculture	3
Energy and utilities	21
Resources and Mining	5
Information Communication Technology	109
Manufacturing	16
Transportation	13
Environment, water and soil	9
Education	19
Financial and insurance services	15
Real estate and insurance services	3
Wholesale and retail trade	6
Legal services	2
Others	56

For participants from organizations that produce ICT products that may be implemented in hardware, firmware, or software confirmed in Q5, we further investigated their adoption of and attitudes towards adopting the Common Criteria through Q8 and Q10 - Q21. Besides the Common Criteria, we explored whether these ICT product manufacturers adopt any other security standards in Q7 and Q9. In addition, the categories that are relevant to the products produced by the participants' organizations were surveyed in Q6.

For the participants whose organizations use ICT products confirmed in Q22, we surveyed if there are any security certification standards the participants' organizations are looking for when they select the ICT products used or to be used within their organizations in Q24 and those certification standards they have obtained in Q25. Specifically, if the organizations use ICT products with Common Criteria certification, the Evaluation Assurance Levels for the products were investigated in Q26. The categories that are relevant to the products used by the participants' organizations were surveyed in Q22. In the absence of ICT products with a security certification standard, by adopting the open-ended questions, we surveyed the ways the participants' manage risks associated with potentially poor implementation of security functionality within the products through Q27 and the ways the participants go about seeking assurances in the security functionality of the products in Q28.

Through various avenues, we distributed the questionnaires and collected the responses from the participants across different countries, organizations, and sectors. To ensure our survey reached a wide range of respondents, we used several strategies to identify potential participants. Firstly, the contact information of participants with a track record of participating in IT security standards was collected from the International Common Criteria Conference website [34]. Secondly, we tried to expand the participants' list by searching users from Common Criteria Users Forum [35], which is a community based around those using the Common Criteria and ISO/IEC 15408 standards. Thirdly, we retrieved the authors from the representative Common Criteria literature (i.e., research paper) as the potential participants and collected their contact details. Furthermore, multiple ICT vendors and companies found in the Common Criteria portal [11] were included to gain a higher response rate of questionnaires. Last but not least, with the support of the Australian Cyber Security Centre (ACSA), the questionnaires were distributed to the ACSA partners [36], which aims to gain the broader viewpoint from participants in the wider cyber security community.

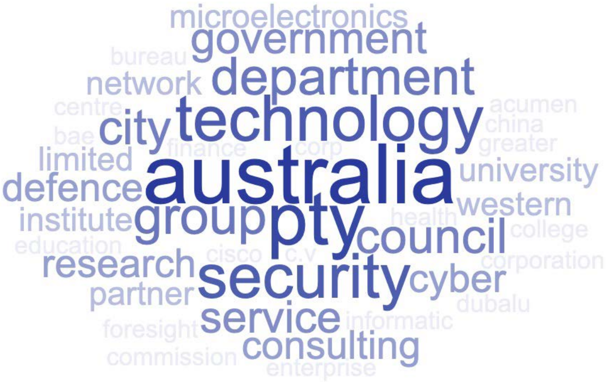

FIGURE 1. Word cloud of the names of participants' organizations that also infer the operating sectors of organizations. The statistics are based on 152 participants of responses who disclosed the name of their organizations. Words that occur frequently appear larger and darker in colour.

Email, Linkedin Message, and blog post [1] were used to reach out to participants interested in cybersecurity standards, which included certification bodies, evaluation laboratories, researchers, policymakers, product developers, sellers, and buyers. Participation in the project is voluntary, and participants are free to stop and skip any question at any time if they do not wish to reveal any specific information. The total number of valid responses was 285, of which 177 answered the entire 28 questions.

B. RESPONSES ANALYSIS

Our participants are from different organizations and sectors, as shown in Table 1. 32.54% of organizations operate in the ICT sector, which is the most significant proportion of participants. Besides the sectors listed in Table 1, including the defence industry, energy and utilities, education, etc., 35.44% of participants chose the "*Others*" option. Based on the analysis of these participants, it appears that most of them are from city councils, police departments, government departments, and national commissions. A few are from consulting and cybersecurity companies, and the others are anonymous participants. To illustrate the range of sectors of the participants, we present the word cloud of the names of participants' organizations based on the responses for Q1 in Figure 1.

[1] https://www.quintessencelabs.com/blog/quintessencelabs-joins-research-study-with-deakin-university-and-charles-stuart-university/

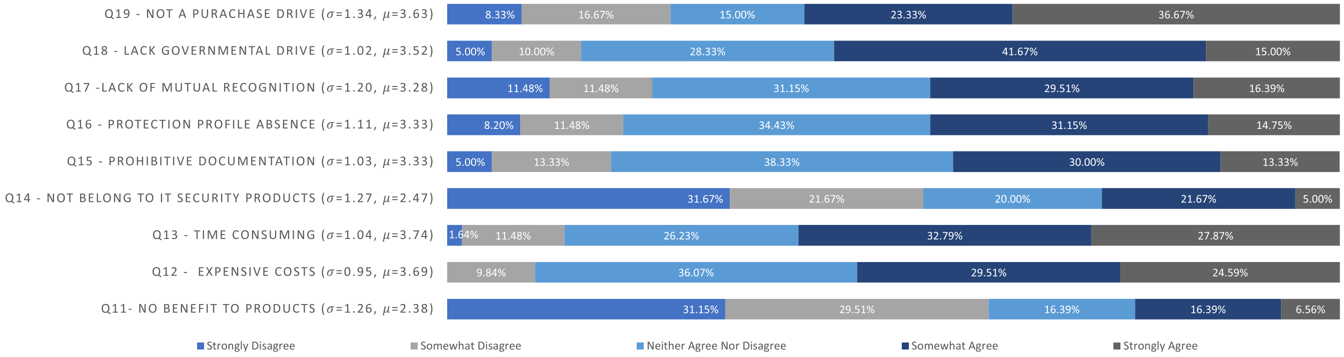

FIGURE 2. The distribution of agreement level for the identified adoption barriers (i.e., Q11 - Q19). The semantic level of agreement is measured using a five-point scale, where each segment represents the probability of respondents who select that level of agreement (*N*=60).

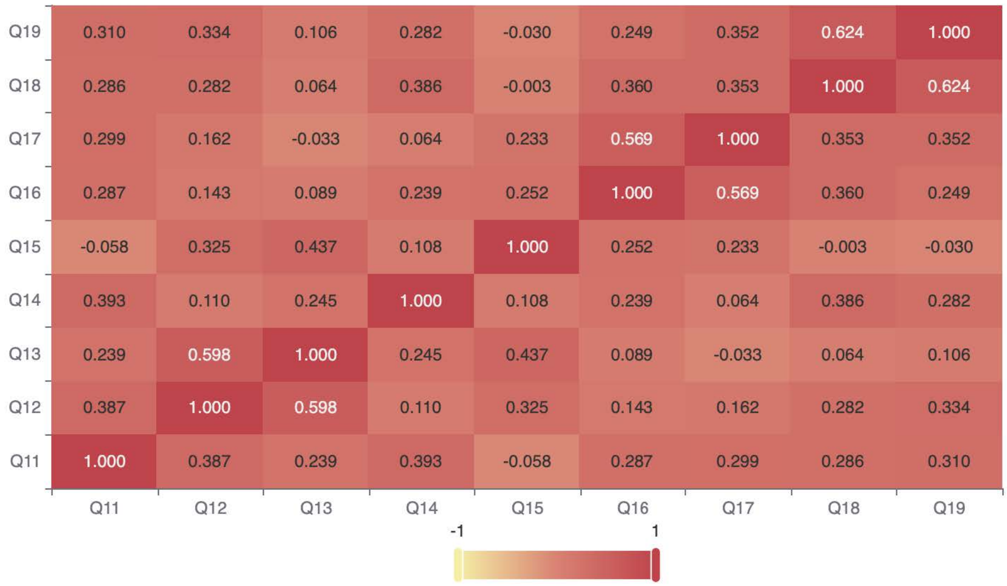

FIGURE 3. Correlation heatmap of the identified adoption barriers (i.e., Q11 - Q19).

Both Australian and international participants are involved in our survey. There are 175 participants' organizations operating in Australia, which takes up 61.40% of the participants. Second place goes to the United States of America, with 11.93%. Besides, organizations operating in Asian, North America, Oceania, South American, and African countries are involved in the survey. Note that these statistics do not reflect the popularity of certifying ICT security products in various countries, but to demonstrate that we made a serious attempt to explore beyond Australia and provide a global picture of the certification adoption landscape.

In addition, from the perspective of the size of organizations, the responses are from organizations with various sizes, including large, mid-market, and small businesses. Among the responses, 37.50% are organizations with more than 1000 employees. Around half (i.e., 46.15%) of the organizations have 11-1000 employees. Besides, there are 16.35% organizations with 0-10 employees participating in our survey from the small business.

For closed-ended questions (i.e., Q11 - Q19) that are designed to investigate adoption barriers of the Common Criteria, based on a five-point scale, we determine the semantic level of agreement for each question using the numbers 1 to 5 to represent strongly disagree to strongly agree. The organizations that produce IT products that can be implemented in hardware, firmware, or software (i.e., the answer to Q5 is Yes) will answer Q11 - Q19. For Q11 - Q19, the number of effective responses is 60. The Cronbach's Alpha tests are conducted to determine the reliability of multiple-question surveys with Likert scales for Q11 - Q19. The Cronbach's α value is 0.749 based on the responses from Q11 - Q19, indicating good reliability and internal consistency [37]. We summarize the quantitative analysis of responses to the closed-ended Q11 - Q19 on the Common Criteria adoption barriers in Figure 2. Specifically, the sample mean (i.e., μ) and standard deviation (i.e., σ) for each question are calculated and shown in 2. Furthermore, the correlation heatmap of the identified adoption barriers (i.e., Q11 - Q19) is displayed in Fig 3. Moderate relationships (i.e., the correlation coefficient is between 0.4 and 0.6) exist between Q12 (i.e., expensive costs) and Q13 (i.e., time consuming), Q16 (i.e., protection profile absence) and Q17 (i.e., lack of mutual recognition), and Q18 (i.e., lack governmental drive) and Q19 (i.e., not a purchase drive).

Lastly, open-ended questions Q20, Q26, and Q27 are designed to explore the Common Criteria incentive strategies and risk management approaches for cyber assurance adopted by the participating organizations in our survey. Since Q20, Q26, and Q27 are exploratory in nature and without hypotheses, the results are described in descriptive form with no statistical comparisons.

IV. OUR FINDINGS

Based on the responses from survey participants,[2] this section describes our findings from the survey on the Common Criteria adoption barriers and the potential incentive strategies to encourage the adoption of the Common Criteria.

A. THE COMMON CRITERIA ADOPTION BARRIERS

We firstly discuss the barriers that discourage organizations from adopting the Common Criteria certification. These adoption barriers are identified from the closed-ended Q11 - Q19 and open-ended Q20. Specifically, we identify the following seven adoption barriers that are common to organizations to answer **RQ1**: (1) absence of technology category in the Common Criteria portal; (2) time consuming and not up-to-date; (3) lack of mutual recognition; (4) lack of security evaluation experience; (5) expensive costs; (6) not a key driver for purchase decisions; (7) lack of governmental drive. These adoption barriers will be discussed in detail below.

1) ABSENCE OF TECHNOLOGY CATEGORY

The Common Criteria uses a framework in which the vendors and purchasers can specify their security functional and assurance requirements for the ICT products. The Common Criteria portal [11] archives the published Protection Profiles and Certified Products under a broad range of categories and diverse technology types. Although the Common Criteria currently cover fifteen categories, there are still 14.75% participants who strongly agree and 31.15% participants who somewhat agree the absence of approved Protection Profiles for the category of the products makes it challenging to obtain the Common Criteria Certification, based on the responses for Q16. In particular, participant with the ID number 2 (P2) specified:

> *"Protection Profiles do not exist for some new technology used by the government such as SD-WAN (i.e., Software-Defined Wide Area Network)".*

In addition, the increasing adoption of emerging technologies motivates the users on bringing in the potential categories of the Common Criteria [38]. The lack of emerging technology category in Common Criteria is an adoption barrier under the reason of absence of technology category. P273 explained:

> *"There is no Common Criteria method for evaluating products which have some security functionality delivered partially or fully from the cloud."*

Components required to operate and manage enterprise ICT environments account for a large proportion of the Common Criteria certified products. For example, according to the statistics on Common Criteria certified products [13], by December 2021, there are 580 certified products under the category of the Integrated Circuits (ICs), smart cards, and smart card-related devices and systems, which takes up the most significant percentage of certified products. However, some organizations found that it is hard to certify their products, compared with the ICT infrastructure products. P22 shared their experiences:

> *"Organization produces building control systems, including HVAC (i.e., Heating, Ventilation, Air Conditioning), Fire & Security, airport management systems, and many IoT products. Historically, the government agencies running the Common Crieria are not interested in these market sectors, remaining focused on infrastructure products to the exclusion of others."*

2) TIME CONSUMING AND NOT UP-TO-DATE

The Common Criteria evaluation process requires a series of stages, including Security Target evaluation, design evaluation, guidance evaluation, life-cycle evaluation, functional testing, and penetration testing. Besides, the evaluation and testing process needs formal documentation following the Common Criteria convention, which takes time to study and compile [39], [40]. On average, the time required for the Common Criteria certification is six months to one-year [5].

More than half of the participants (60.66%) agree that the Common Criteria evaluation time is too long compared to the product life cycle (Q13). For products that have a short time-to-market, the lengthy evaluation period hinders the adoption of the Common Criteria. To illustrate, P16 shared their experience on Common Criteria certification:

> *"Another factor hindering Common Criteria adoption is that the approval is only for a specific release, which is years old by the time certification is obtained... There should be a path to quickly have a new version accepted for certifications."*

As technology changes rapidly, the time-consuming process of Common Criteria evaluation and certification impedes the commercialization of security products in the market. As an example, when the Common Criteria certification process concludes, the technology for manufacturing low-cost IoT devices may have become obsolete. Customers may expect the latest features instead of absolute security assurance. As a proof, P125, as one of the largest multi-disciplinary insurance agencies in Australia, said: *"Clients want latest features, these haven't time for Common Criteria evaluation prior to release... "*. P273 from the telecommunications equipment company had similar concerns: *"The software*

[2] The IDs of participants are used to refer to the survey participant (P).

release cadence of cloud products (e.g., monthly) would not align with Common Criteria certification time-frames."

3) LACK OF MUTUAL RECOGNITION

The Common Criteria is the driving force for the widest available mutual recognition of secure ICT products. As of 2021, there are 17 certificate authorizing schemes under the Common Criteria [41]. Country-specific implementation of Common Criteria schemes are different in the flow of evaluation and certification of ICT products [19]. The fragmented landscape of Common Criteria schemes generates the disharmonized perspective for security evaluation. In particular, the US keeps the certified products listed for two years before being archived, while the other counties keep them for five years. Nearly half (45.90%) of our participants agree that there is a lack of mutual recognition on Common Criteria certification among the countries where your products are sold (Q17). P273 emphasized the different lifetimes for different schemes, *"Different schemes enforce different certificate lifetimes, e.g., NIAP - 2 years, Canada - 5 years etc."*

The lack of mutual recognition across diverse security standards is one adoption barrier for security certifications, including the Common Criteria [5]. The comment from one of the ICT product consumers P103 remarked *"Certification overload makes anyone choice hard."* Harmonization of the certification results across different standards is expected from both consumers and vendors to improve the transparency of the security certifications. As the vendor, P16 stated:

> *"No commonality among related certifications. Why can't testing for FIPS 140-3 be accepted as testing for NDcPP? Why can't NDcPP testing be accepted for EAL2? Why can't NDcPP and EAL2 be combined? I would like to see a requirement table which showed relationships between EAL2, NDcPP, FIPS 140-3, EU Cybersecurity law, California Cybersecurity law… "*

4) LACK OF SECURITY EVALUATION EXPERIENCE

The Common Criteria standard is somewhat complex and not easy to follow to conduct evaluation in terms of its usability and readability. For example, participant P147 commented *"unclear on the process to undertake evaluation"*, P4 stated *"internal resources unavailability"*, and P14 recommended that *"streamline Common Criteria adoption process will be helpful."* 43.33% of our participants agreed that the documentation requirements for Common Criteria evaluation are prohibitive, so that it is difficult to obtain the Common Criteria certification (Q15). In response, many product vendors engage consultants to prepare specific evaluation material at the pre-evaluation stage. The current efforts on major review work are underway by international experts through the International Organization of Standardization (ISO) [19]. This should see an improvement of the Common Criteria for wider adoption from the perspective of usability and readability of the documentation.

However, updating and revising the Common Criteria make the certification process inconsistent when users intend to obtain a Common Criteria certification. A few national evaluation schemes are phased out of using Evaluation Assurance Levels (EALs) and only accept products that claim strict conformance with Protection Profiles approved by them. In fact, only Protection Profile evaluations are currently allowed in the United States. P18 mentioned this difficulty when they tried to certify their product under a particular Common Criteria scheme: *"Lack of consistency and changing rules in the middle of an evaluation makes it very difficult to properly plan and evaluate our products."*

Furthermore, it is not within the scope of the Common Criteria to detail how cryptography is implemented within the TOE. Instead, national standards, such as FIPS 140-2 [42], specify the specifications for cryptographic modules, and various standards specify the cryptographic algorithms used. In recent years, the Protection Profile authors have included cryptographic requirements for Common Criteria evaluations that would generally be covered by FIPS 140-2 evaluations, expanding the scope of the Common Criteria by using scheme-specific interpretations.

In addition, a common phenomenon of the security evaluation is the lack of talent and expertise, especially Common Criteria. The outflow of talent with the security evaluation expertise is happening. According to the response from an Australian technology company P152:

> *"…New entrants don't see a career path and prefer to work out how to leave as soon as possible…A small core remains in security evaluations."*

5) EXPENSIVE COSTS

In our survey, 24.5% of participants strongly agree, 29.5% somewhat agree, and no participant strongly disagrees that the Common Criteria evaluation costs are too expensive compared to the benefits brought into the evaluated products (Q12). The evaluation costs to obtain the Common Criteria certification is commonly regarded as a barrier to the Common Criteria certification adoption [5], [43], particularly for companies with a limited budget and low-margin products. ICT products with a low-profit margin may not be able to justify and defray the costs associated with Common Criteria certification, given the market's competitive nature. Based on the investigation on certified products listed on the Common Criteria portal [44], the Common Criteria certification is relatively more likely to be adopted by companies with a high-profit margin and capable of sustaining sensitive government networks. P96 shared their thoughts on the cost of Common Criteria evaluation:

> *"Common Criteria (and its predecessor) was a nice idea but has always been too expensive… "*

Generally, in line with the Australia scheme, obtaining the Common Criteria certification involves four steps:

pre-evaluation, *conduct*, *conclusion*, and *assurance continuity*. In the first step, *pre-evaluation* is essential to ensure the success of the Common Criteria evaluation process, prevent delays, conduct initial assessments, develop the Security Target and the evaluation schedule. This includes the writing of functional, high-level, and low-level design specifications. As a second step, the *conduct* phase verifies any claimed security functionality under the Common Criteria, and any other claimed cryptographic functionality under the specific security standard, such as FIPS 140-2 [45]. The evaluation and certification processes are finalized in the *conclusion* phase. Additionally, *the assurance continuity* phase allows for a minimization in the number of evaluations and the options of extending certification to the updated Target of Evaluation version.

In general, the costs of an evaluation depends on the security assurance level or Protection Profile conformance claims, as well as on the complexity of the Target of Evaluation [46]. A start-up database company P45 commented on the cost of Common Criteria evaluation:

> *"We've learnt that the certification cost may be above 100k USD, which is too expensive for startups or companies in early developing stages, like ours."*

The overall evaluation costs are composed of four components: *internal costs*, *external costs*, *lab fees*, and *certification fees*. The *internal costs* are incurred on preparing deliverables and supporting the evaluators. The *external costs* consist of consultancy fees. The *lab fees* are paid to the evaluation labs, and the *certification fees* are paid to the corresponding certification body if applicable. The cost of conducting complex evaluation activities in laboratories is substantial. A recently estimated average cost for a Common Criteria certification lifecycle is US$250,000 [5] depending on the evaluation assurance level and re-use of past evaluation effort. The cost of an evaluation against a Protection Profile is relatively inexpensive due to the reduced efforts in developing the evaluation documentation. Because of the heavy cost on the Common Criteria lifecycle, it is challenging to evaluate the products against the Common Criteria standard for organizations.

6) NOT A KEY DRIVER FOR PURCHASE DECISIONS

A majority of the participants (60.66%) strongly or somewhat disagree with the statement in Q11: Common Criteria certification does not add any benefits to your products. However, when considering issues related to the economic viability of the organizations, 36.67% of our participants strongly agree that Common Criteria certification seems not to be a key driver for purchasing decisions of commercial customers (Q19). For example, P147 said: *"Unclear on the value it would provide to the business."*

For start-up companies or low-margin businesses, the budget for gaining security certifications is limited. As a participant from a start-up company, P27 realized that the organization should take countermeasures to cope with cyber attacks. However, the highest priority for spending time and money is on delivering new functionality:

> *"...As a startup, our focus is on adding additional functionality and must-have features than on optional ones... Our customers are not that security-focused."*

Additionally, some organizations expect to gain economic benefits from Common Criteria certification in addition to security assurance. P27 further put it: *"It is difficult to forecast revenue associated to a certification to justify certification expenses."* P112 pointed out that the decision to pursue Common Criteria certification for their products is partly determined by market demand:

> *"Certification of a product must contribute to the commercial viability of the product. This should be done by a combination of measures to change the cost/effort barrier to achieving product certification and to improve the unit price/accessible market/demand for the certified product."*

7) LACK OF GOVERNMENTAL DRIVE

Within the Q18 respondents, 28% strongly or somewhat agree that there is a lack of governmental drive (e.g., security certification requirements) in their procurement policy for the Common Criteria certification. P111 commented: *"People once cared about Common Criteria certification, but the current PSPF (i.e., Protective Security Policy Framework)/ISM (i.e., Information Security Manual) really don't encourage us."* Some organizations found it hard to seek help and support from government agencies, such as the input from P112:

> *"Government and commercial do not see product certification as a key part of the risk management around the selection and implementation of effective security controls. Government agencies are very unhelpful in establishing any form of commercial justification to get a product certified and in getting products through any form of the certification process."*

B. ADOPTION OF THE COMMON CRITERIA: RECOMMENDATIONS

According to the response received from our survey participants, the above identified barriers hinder the adoption of the Common Criteria. Security standards have always been considered an effective way to provide cyber assurance, although there are some obstacles to widely embracing these security standards. To drive the broad adoption of the Common Criteria and the wider range of security standards, we next discuss the identified Common Criteria incentive strategies and summarize six categories as follows in responding **RQ2**: (1) guidance, resources, and expertise; (2) governmental incentive; (3) mutual recognition; (4) procedure optimization; (5) extension into emerging technologies; (6) consumers' trust.

1) GUIDANCE, RESOURCES, AND EXPERTISE

The guidance and resources on how to begin the Common Criteria assessment process, including developing Protection Profile, preparing Security Target, and testing for evaluation, are highly desirable. Although there are documents that introduce the Common Criteria general model [47], security functional requirements [48], and security assurance requirements [49] available on the Common Criteria portal [11], many participants found it is hard to initiate the procedures due to the lack of usability and readability of these documents as identified in Section IV-A4. For example, P147 emphasized the need for *"better guidance on when a product should be evaluated, and how to begin the process."*

Besides the Common Criteria portal, another important source of information is the International Common Criteria Conference (ICCC) [34]. It is a technical conference where professionals involved in the Common Criteria exchange their experiences in specification, development, evaluation, certification and approval with regard to the ICT security of products and systems. Although the ICCC is held annually for the community of professionals involved in Common Criteria, the experiences shared on the process of Common Criteria assessment are hard to access through public resources. Based on the situation, some companies choose to utilize *"outsourced service"* (P4) that transfers the tasks to professionals with Common Criteria expertise. Moreover, some companies choose to establish their own information bank. P147 shared their approaches on how to accumulate guidance, resources, and expertise on the Common Criteria:

> *"[Company name] has its own training material and induction process for trainee evaluators. This material includes specific examples of EAL2+ assurance classes and evaluations. A training package that included completed examples of EAL2+ (including ALC_FLR.2) assurance classes "which was intended to be shared with TOE developers" would be ideal as it will allow new entrants to view and understand the source material required as inputs to the assurance classes. It would also allow new [Company name] workers to view and create templates to speed up the creation of assurance classes."*

2) GOVERNMENTAL INCENTIVE

According to the responses from our participants, government supports and incentives motivate the adoption of Common Criteria evaluations and Common Criteria certified products to a certain extent. As the manufacturers of ICT products, some participants adopt the Common Criteria to meet the government's procurement requirements in order to access the markets. For example, P273 shared one of the reasons for adopting Common Criteria evaluations:

> *"As an IT equipment manufacturer, [Company name] adopts the Common Criteria as a market access requirement for various government markets globally."*

Consumers of Common Criteria certified products can be categorized based on market sectors: public and private. When it comes to the public sector, government supports can boost the adoption of Common Criteria certifications through the requirement of Common Criteria certified products. For example, establishing policy requirements for the procurement process used by government departments and agencies encourages the Common Criteria adoption. The US government requires Common Criteria certified products for specific applications. This policy encourages vendors to participate in Common Criteria evaluations [46]. P103 shared the ideas on the Common Criteria incentive strategies: *"Government mandate or engagement, critical mass in the market."* Similar comments came from P274 and P27: *"Governments mandate for customer and assistance to vendors to get started"* (P274), *"Government regulation"* (P27).

In addition, government incentives can encourage the adoption of Common Criteria certified products in the private sector. The government's support and incentives would be essential in boosting the uptake of Common Criteria certifications since the vendors could minimize legal risks and gain economic benefits from performing the Common Criteria evaluations. For instance, in Japan, tax deductions are available for businesses that use Common Criteria certified products, which increases the purchase of the certified products [50]. *"Government funding"* (P106), *"Government grants"* (P100), *"Sponsorship from government"*(P61) and *"Tax incentive"*(P3) were proposed to encourage the adoption of the Common Criteria from our participants for responding Q21 - What kind of incentive would be helpful for your organization for adopting Common Criteria certification.

3) MUTUAL RECOGNITION

Globally, there are a variety of cybersecurity standards, including international, national, and industry-specific regulations. Comparing the level of security between different standards is difficult. As P44 stated: *"There are many security certification standards."*. Even for the single Common Criteria standard, it is difficult to achieve the objective of comparability due to the technical nature of the document [5]. To achieve the objective, it was proposed to establish a single comprehensive standard to facilitate mutual recognition among various security standards. For example, P189 remarked:

> *"I think a mass move toward a single comprehensive standard within [Country name] would strongly influence my organization to re-evaluate the need to maintain a standard that essentially duplicates effort and paraphrases similar criteria to other standards."*

Evaluation in the future can be made more comparable and harmonized by standardizing evaluation activities.

For product comparability, rigorous security metrics can be developed that indicate the level of threats, risks, and security provided by each.

4) PROCEDURE OPTIMIZATION

Through unified processes and formalized steps, evaluation activities are made more manageable. For example, P159 expected *"Lower barriers to entry and a quicker, more transparent process"* to adopt the Common Criteria. Usually, implementation-independent Protection Profiles in the Common Criteria [51] define the security requirements for ICT technology that consumers expect. Independent laboratories then evaluate products to decide if the claimed security properties have been achieved [52]. Standardization of evaluation and testing procedures in the future will make the certification process more transparent.

In addition, *"the agile and swift"* (P14) process can be considered as the future direction of the optimization procedure for the Common Criteria. Many participants are expecting the *"faster timeframes"* (P130), *"faster pace with faster path for features updates"* (P156) for the Common Criteria certification. In order to respond quickly with rapid iterations and updates on technology, the Common Criteria need to be continuously updated with requirement discovery and solution improvement through the collaboration of vendors, technical specialists, customers, and governments.

Lastly, our participants are concerned about the costs associated with Common Criteria evaluation and certification, as mentioned in Section IV-A5. There are several proposed ways of reducing the cost proposed, including *"Reducing gap analysis cost, consulting cost, evaluation voucher, etc."* (P10), *"Free evaluations for two products per company."* (P125), and governmental supports discussed in Section IV-B2.

5) EXTENSION INTO EMERGING TECHNOLOGIES

ICT security-related technologies and evaluations are covered by the Common Criteria, from functionalities to security assurance. Traditional ICT technology and products, such as ICs, database and network devices, are sufficiently covered and evaluated under the Common Criteria standard in the past decades [6]. In light of emerging technologies, the Common Criteria standard needs to address the evaluation of new technologies, such as blockchain, quantum computing, artificial intelligence, and IoT. This is confirmed by P22 who indicated the importance of: *"extension into IoT and commercial sectors."* Additionally, privacy laws should be observed for high assurance products, such as privacy-preserving authentication.

6) CONSUMER TRUST

The adoption of security-sensitive ICT products relies heavily on the trust the users' place in the security features of these products. The trust of users are considered the driving force behind certifications and cybersecurity standards. P41 stated:

> *"Adopting Common Criteria certification or not is up to the commercial customers in the target market of the products."*

Assuring the security of ICT products is a joint endeavour between vendors, technical specialists, customers, and governments that never ends. Through education and information available on the Common Criteria portal [11] and other platforms, sharing information on the core blocks of Common Criteria evaluation and certification will contribute to this cause. The trustworthiness of ICT products and the Common Criteria can be established if consumers are provided with long-term security assurances regarding the products' security features. C150 identified other factors that influence the purchase of security-enhanced ICT products, aside from certification:

> *"From the perspective of a consumer of security products, Common Criteria (or similar) is not a factor. It is the real world efficacy of a security product combined with the ability to readily implement, maintain and manage that influence the purchasing decision, not a certification."*

The implementation of security-by-design in product engineering processes can not only significantly shorten the evaluation and certification process, but also ensure that products are designed from the very beginning to be secure [53]. The incremental certification of products for additional functionality and features will be more accessible with the integration of certification and evaluation into the product development process [54], [55]. Furthermore, the certification itself, accompanied by continuous assurances of products' security to consumers, helps consumers build and strengthen trust in the Common Criteria.

V. RISK MANAGEMENT DIRECTIONS FOR CYBER ASSURANCE

By investigating Common Criteria adoption barriers, we understand the process of organizations making decisions when they purchase, produce, and use ICT products with security functionalities. In addition to adopting security standards such as the Common Criteria as discussed in Section IV, there are other risk management approaches to achieve cybersecurity assurance that organizations can take to protect their assets and the data of their employees, business partners, and customers. We further discuss our investigation of risk management approaches for cyber assurance adopted by the participating organizations in our survey with the proposed future directions for risk management of organizations to address **RQ3**. The analysis is based on the responses in Q26 and Q27, which are open-response survey questions about risk management and cyber assurance. As the study is exploratory, we have no hypotheses and conduct no statistical comparisons in this section.

A. REACTIVE VS PROACTIVE CYBERSECURITY

An organization can choose to take a proactive approach to cybersecurity, preventing threats before they arise, or a reactive approach, addressing cybersecurity breaches after they have occurred. Reactive cybersecurity investigates the signs that indicate a data breach has occurred and a cybersecurity incident has been committed [56]. The reactive approach involves responding to cybersecurity incidents in case of further damage [57]. Proactive cybersecurity investigates the indicators of compromise, which is a broad and overall approach that involves not only specific methods and practices but also a mindset of protecting cybersecurity before the incidents happen in advance [3]. Below, we categorize the cybersecurity risk management approaches shared by our participants and analyze these approaches from the reactive and proactive points of view respectively.

1) PATCH MANAGEMENT

Patching falls under the Essential Eight in the Strategies to Mitigate Cyber Security Incidents of the Australian Cyber Security Centre [58]. Patch management is applied to computer systems, applications, cloud infrastructure, and other critical infrastructure (e.g., industrial control systems) to mitigate cybersecurity incidents. Once a vendor releases a patch, the patch should be applied in a timeframe commensurate with an organization's exposure to the security vulnerability and the level of cyber threat the organization is aiming to protect itself against. Once a newly discovered security vulnerability in an internet-facing service is made public, adversaries will likely develop malicious code within 48 hours [59].

Some of our participants handled patching management in their own way. For example, P229 mentioned that they conducted *"regular review of available updates and patching"* as part of the risk management process, and P134 reviewed *"patch management forums"* to check the feedback on the products prior procurement. A reactive patch is applied in response to an issue that currently affects a system and that needs immediate relief [60]. When such a situation occurs, users typically install the most recent patch or patches, which may appear to be capable of resolving the issue. However, in many cases, problems that can occur have already been identified, and patches have already been released. Compared to a reactive patch management strategy, a proactive patch management strategy implies more changes and regularly scheduled maintenance windows to reduce unplanned issues [61].

2) CYBER RISK PROFILE

The cyber risk profile is a quantitative approach for assessing cybersecurity risks for an organization, asset, project or individual [62]. In the absence of cybersecurity certifications, some participants establish a risk profile for the product to manage risks. For example, P193 shared their experience on how to manage risks when there are no cybersecurity certifications for the products:

> *"...We establish an overall risk profile for the product to consider what information will be stored, processed or communicated using the product, as well as establishing mitigating or alternative controls to manage the absence of the certification."*

As a reactive way, the audit data can be retrieved to avoid further damage if cybersecurity incidents have happened [63]. Furthermore, the risks are monitored based on the established risk profile. For example, P140 mentioned that the risks are monitored in *"the lifecycle of the supportability of the product"*. The procedures and countermeasures are formulated based on the risk profile to understand the risks, assess them, and mitigate them. Therefore, the organization proactively manages the risks on products, systems, assets, and projects to reduce the likelihood of cyber attacks, as illustrated by P156's example:

> *"Evaluate the risk profile versus benefit for the product in question and put in place commensurate controls and standard operating procedures to minimize the security risk."*

It is worth mentioning that through the secure sharing of risk profiles across organizations, the information on risk management can be shared to improve cyber resilience. For example, the Open Science Cyber Risk Profile (OSCRP) aims to help improve IT security for open science projects [64] for scientists and IT professionals, which serves to bridge the communication gap between scientists and IT security professionals and allows for the effective management of risks to open science caused by IT security threats.

3) SELF AND IN-HOUSE EVALUATIONS

Independent testing, such as *"penetration testing"* (P11), *"own vulnerability scanning"* (P125), *"in-house examination"* (P104), was adopted by our survey participants for cyber assurance based on the survey. Through independent testing, ICT products are tested with white-hat hackers to find exploitable vulnerabilities. In addition, potential exploits can be closed with the help of penetration testing in the proactive approach. The mitigation recommendations and strategies will be decided to conduct risk management within organizations based on the testing results. P273 shared their experience on their self and in-house evaluations:

> *"For cloud products, we conduct a detailed cloud security assessment based on the business criticality of information classification of its use within [Company name]. For on-prem products, we conduct in-house evaluations prior to deployment."*

4) CYBERSECURITY INSURANCE

Cyber risk management is imperative due to the significant economic impacts and increased media attention [30]. In the light of the need for improving risk management within organizations, cybersecurity insurance companies have been developing steadily in recent years [65]. For instance, BizCover [66] is an insurance company that will cover expenses on cybersecurity incidents. In the context of cybersecurity insurance, the cyber risk is tagged with a price, which creates incentive for risk-appropriate behavior. In addition, by simply applying for cybersecurity insurance, the organizations become more aware of self-protective awareness against the cyber threats. Cybersecurity insurance assists users in taking a proactive approach to cybersecurity in addition to potentially covering the financial cost of dealing with cybersecurity attacks in the reactive way [67].

Some of our participants, especially small businesses, chose to use insurance companies to seek assurances in the cybersecurity aspect. For example, P7 is a global IT company with the size between 51-250 employees mentioned that they employed *"insurance companies"* to manage risks associated with potentially poor implementation of security functionality within the products in the absence of IT products with a security certification standard and used *"insurance companies"* to seek cyber assurance.

However, there are a number of difficulties that restrict the development of cybersecurity insurance, including loss occurrence, information asymmetries, and the limits of insurance coverage [30]. With the increasing market development, the risk information pool for cybersecurity insurance will become more extensive with more available data. Therefore, sharing data through national regulators or international associations will improve insurance risk assessments and insurance market efficiency.

5) CYBERSECURITY AWARENESS EDUCATION

According to MediaPRO's annual privacy and security awareness report, 85% of finance workers lacked knowledge around data privacy and cybersecurity [68]. Besides the professional education on evaluation as introduced in Section IV-A4, cybersecurity uncertainty will be mitigated by keeping employees up to date on the latest threat intelligence and attack methods. In addition to reducing stress, security training helps eliminate risky behaviours and establishes a culture of cybersecurity in the workplace regarding security standards.

Based on the responses from our questionnaires, many organizations provided cybersecurity training to their staff to establish their awareness. For example, P67 said that they offered *"policies/procedures and staff cybersecurity training"*, and P229 shared that they trained their staff with *"industry best practices guides"* and *"previous implementation experience."*

Besides the training on cybersecurity standards, the best practices, and standards, making sure users know how to spot the tell-tale signs and tricks of fraudsters will enable them to avoid social engineering and other phishing attacks.

B. MULTI-LAYERED RISK MANAGEMENT

Although a few participants indicated that *"never attempted to"* (P3) seek cybersecurity assurances with the product and *"not used"* (P246) risk management. In most cases, our participants took steps to ensure cybersecurity and prevent potential threats. Rather than relying on a single approach to managing risks, most of our participants adopted multiple risk management strategies. For example, P262 introduced how to obtain cyber assurance within the organization when accessing the ICT products:

> *"For products and services that we have access to, we will use a mix of audit and technical testing capabilities to obtain an appropriate level of assurance. The degree of this activity is dependant on the risk."*

In order to effectively manage risk, organizations need a systemic multi-layered approach that crosses multiple business units, departments and processes, touching every individual, machine and element within the organization. Below, we discuss how to obtain cyber assurance through the multi-layered risk management based on the responses from our participants.

Firstly, in the process of product design and implementation, practical risk management tools and approaches are employed through assurance activities. For example, P78 mentioned that they utilized *"vulnerability management and mitigation controls where possible"* to manage risks within the products during the product implementation process. Organizations also follow *"best practices recommended by governments"* (P267) and *"industry best practices guide"* (P229) in this process, such as the implementation of security-by-design as demonstrated in Section IV-B6. P119 shared their activities in this process:

> *"Through detailed threat modeling and analysis and designing required mitigations. Standard cybersecurity risk management practices are then used as a mechanism to provide required assurance."*

Secondly, organizations need to protect their cybersecurity and improve their cyber resilience when selecting and utilizing these ICT technologies. Usually, organizations combine a number of available data to choose ICT products. Many participants preferred to choose products with *"trusted brands"* (P143) and *"reputable companies"* (P75). Besides reference checks on the products, security certification is an essential element to check for the purchasers. For example, P83 declared: *"We need to see the certification from the vendors"*. In addition, some participants conducted *"own independent testing"* (P159) or *"3rd party efficacy test"* (P150) before procurement and monitor the products during use. P57 shared their activities before procurement to achieve cybersecurity assurance:

> *"Generally achieved through supply chain due diligence, selecting preferred and trusted suppliers and by conducting internal assessment and suitability validation of the products as fit for purpose and being with the risk thresholds of the organization."*

Thirdly, cybersecurity attacks and incidents are inevitable nowadays. Organizations prepare for the worst before incidents occur and try their best to reduce losses if incidents have already occurred. Another layer of risk management relates to incident management. Audit data should be traceable to help organizations reflect on the attacks to avoid similar attacks in the future. Some of our participants chose to utilize an insurance company as shown in 5.1.4. In addition, setting up a response team to prepare for mitigation recommendations and actions is necessary to bounce back after cybersecurity incidents.

Furthermore, cybersecurity issues are not limited to the IT department. They pose a significant threat to business continuity and reputation and threaten every aspect of an organization. Security awareness within the company helps employees understand cyber hygiene that refers to the practices for ensuring the safe handling of data and for securing networks [69]. Educating employees about the security risks associated with their actions via email and the web reduces the chances of being attacked [70]. As demonstrated in 5.1.5, some of the staff from the organizations of our participants were provided with cybersecurity training. Furthermore, since cybersecurity is a cross-functional concern, the organizations sometimes need to work with external entities to share information on cybersecurity to improve cyber resilience. Hence, besides cybersecurity awareness education, the C-suite level plays an imperative role in establishing a cybersecured organization [71].

VI. CONCLUSION

In this work, we presented the results of our survey on the Common Criteria adoption and approaches to ensuring cyber assurance for organizations. To determine if organizations have concerns related to cybersecurity regulatory issues as well as to determine organizations' attitudes towards being measured against cybersecurity standards, seven adoption barriers of security standards and certifications are identified. The results of our study inform our recommendations for promoting Common Criteria adoption and broader cybersecurity standards and certifications. Aside from the use of cybersecurity standards and certifications to select secure ICT products, we investigate how organizations pursue cyber assurance and their adopted strategies. We hope the findings and recommendations we have made help researchers, organizations, and regulators raise concerns among academia and industry about the importance of cybersecurity standards and certifications. Beyond cybersecurity standards and certifications, the survey presents insights and directions on risk management, in the hope of inspiring organizations to achieve cyber assurance.

REFERENCES

[1] Delltechnologies Technologies. (2020). *Four Keys to Navigating the Hardware Security Journey*. [Online]. Available: https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-four-keys-to-navigating-the-hardware-security-journey.pdf

[2] Australian Cyber Security Centre. (Sep. 2020). *ACSC Annual Cyber Threat Report*. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-CyberThreat-Report-2019-20.pdf

[3] N. Sun, J. Zhang, P. Rimba, S. Gao, Y. Xiang, and L. Y. Zhang, "Data-driven cybersecurity incident prediction: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1744–1772, 2nd Quart., 2018.

[4] Australian Cyber Security Centre. (Sep. 2021). *ACSC Annual Cyber Threat Report*. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

[5] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "A survey of cybersecurity certification for the Internet of Things," *ACM Comput. Surv.*, vol. 53, no. 6, pp. 1–36, Nov. 2021.

[6] D. S. Herrmann, *Using the Common Criteria for IT Security Evaluation*. Boca Raton, FL, USA: CRC Press, 2002.

[7] N. Sun, C.-T. Li, H. Chan, B. D. Le, M. Islam, L. Y. Zhang, M. Islam, and W. Armstrong, "Defining security requirements with the common criteria: Applications, adoptions, and challenges," *IEEE Access*, vol. 10, pp. 44756–44777, 2022.

[8] Common Criteria. (Apr. 2017). *Common Criteria for Information Technology Security Evaluation—Part 1: Introduction and General Model*. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf

[9] Licensed Laboratories. (Feb. 2021). *Common Criteria*. [Online]. Available: https://www.commoncriteriaportal.org/labs/

[10] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, *Computer Security: Principles and Practice*. Upper Saddle River, NJ, USA: Pearson, 2012.

[11] Common Criteria. (2021). *The Common Criteria Portal*. [Online]. Available: https://www.commoncriteriaportal.org/

[12] J. Hearn, "Does the common criteria paradigm have a future?" *IEEE Secur. Privacy Mag.*, vol. 2, no. 1, pp. 64–65, Jan. 2004.

[13] Common Criteria. (2021). *Certified Products List—Statistics*. [Online]. Available: https://www.commoncriteriaportal.org/products/stats/

[14] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids—A comprehensive survey," *Comput. Standards Interfaces*, vol. 56, pp. 62–73, Feb. 2018.

[15] M. Kara, "Review on common criteria as a secure software development model," *Int. J. Comput. Sci. Inf. Technol.*, vol. 4, no. 2, p. 83, 2012.

[16] M. Bures, T. Cerny, and B. S. Ahmed, "Internet of Things: Current challenges in the quality assurance and testing methods," in *Proc. Int. Conf. Inf. Sci. Appl.* Singapore: Springer, 2018, pp. 625–634.

[17] J. P. Dias, F. Couto, A. C. R. Paiva, and H. S. Ferreira, "A brief overview of existing tools for testing the Internet-of-Things," in *Proc. IEEE Int. Conf. Softw. Test., Verification Validation Workshops (ICSTW)*, Apr. 2018, pp. 104–109.

[18] I. Kuzminykh and A. Carlsson, "Analysis of assets for threat risk model in avatar-oriented iot architecture," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Cham, Switzerland: Springer, 2018, pp. 52–63.

[19] M. Fatima, H. Abbas, T. Yaqoob, N. Shafqat, Z. Ahmad, R. Zeeshan, Z. Muhammad, T. Rana, and S. Mussiraliyeva, "A survey on common criteria (CC) evaluating schemes for security assessment of IT products," *PeerJ Comput. Sci.*, vol. 7, p. e701, Oct. 2021.

[20] A. Barabanov and A. Markov, "Modern trends in the regulatory framework of the information security compliance assessment in Russia based on common criteria," in *Proc. 8th Int. Conf. Secur. Inf. Netw.*, Sep. 2015, pp. 30–33.

[21] A. Barabanov, A. Markov, and V. Tsirlov, "Russian it security certification scheme: Steps toward common criteria approach," in *Proc. 15th Int. Common Criteria Conf. (ICCC)*, New Delhi, India, 2014, pp. 1–11.

[22] L. Hu, H. Li, Z. Wei, S. Dong, and Z. Zhang, "Summary of research on IT network and industrial control network security assessment," in *Proc. IEEE 3rd Inf. Technol., Netw., Electron. Autom. Control Conf. (ITNEC)*, Mar. 2019, pp. 1203–1210.

[23] Australia Cyber Security Centre. *Security Risk Management*. Accessed: Jan. 3, 2022. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/glossary/security-risk-management

[24] K.-K.-R. Choo, K. Gai, L. Chiaraviglio, and Q. Yang, "A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management," *Comput. Secur.*, vol. 102, Mar. 2021, Art. no. 102136.

[25] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: A review and research agenda," *Supply Chain Manage., Int. J.*, vol. 25, no. 2, pp. 223–240, Nov. 2019.

[26] F. Hoppe, N. Gatzert, and P. Gruner, "Cyber risk management in SMEs: Insights from industry surveys," *J. Risk Finance*, vol. 22, nos. 3–4, pp. 240–260, Nov. 2021.

[27] J. Meszaros and A. Buchalcevova, "Introducing OSSF: A framework for online service cybersecurity risk management," *Comput. Secur.*, vol. 65, pp. 300–313, Mar. 2017.

[28] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, Jul. 2014.

[29] A. Ahmad, S. B. Maynard, K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville, "How can organizations develop situation awareness for incident response: A case study of management practice," *Comput. Secur.*, vol. 101, Feb. 2021, Art. no. 102122.

[30] C. Biener, M. Eling, and J. H. Wirfs, "Insurability of cyber risk: An empirical analysis," *Geneva Papers Risk Insurance-Issues Pract.*, vol. 40, no. 1, pp. 131–158, Jan. 2015.

[31] H. I. Kure, S. Islam, M. Ghazanfar, A. Raza, and M. Pasha, "Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system," *Neural Comput. Appl.*, vol. 34, pp. 1–22, Aug. 2021.

[32] S. Laube and R. Böhme, "Strategic aspects of cyber risk information sharing," *ACM Comput. Surveys*, vol. 50, no. 5, pp. 1–36, Sep. 2018.

[33] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018.

[34] (2021). *International Common Criteria Conference*. [Online]. Available: https://iccconference.org/

[35] *Common Criteria Users Forum: CCUF Portal*. Accessed: Jan. 3, 2022. [Online]. Available: https://www.ccusersforum.org/

[36] Australia Cyber Security Centre. *Partner Hub*. Accessed: Jan. 3, 2022. [Online]. Available: https://www.cyber.gov.au/partner-hub/overview

[37] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," *Int. J. Med. Educ.*, vol. 2, p. 53, Jun. 2011.

[38] N. Sun, B. D. Le, C.-T. Li, W. Armstrong, I. M. Zahidul, I. M. Rafiqul, L. Y. Zhang, and H. Chan, "Review on common criteria adoptions and challenges in protection profile development for encryption technologies," Cyber Secur. Cooperat. Res. Centre, Joondalup, WA, Australia, Tech. Rep. DACCA–D1, Mar. 2020.

[39] S. P. Kaluvuri, M. Bezzi, and Y. Roudier, "A quantitative analysis of common criteria certification practice," in *Proc. Int. Conf. Trust, Privacy Secur. Digit. Bus.* Cham, Switzerland: Springer, 2014, pp. 132–143.

[40] S. J. Murdoch, M. Bond, and R. Anderson, "How certification systems fail: Lessons from the ware report," *IEEE Secur. Privacy*, vol. 10, no. 6, p. 40, Nov. 2012.

[41] Common Criteria. (2021). *Certificate Authorizing Schemes*. [Online]. Available: https://www.commoncriteriaportal.org/ccra/schemes/

[42] *FIPS 140-2 Validation Certificate*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2009.

[43] G. Baldini, A. Skarmeta, E. Fourneret, R. Neisse, B. Legeard, and F. Le Gall, "Security certification and labelling in Internet of Things," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 627–632.

[44] Common Criteria. (2021). *Certified Products*. [Online]. Available: https://www.commoncriteriaportal.org/products/

[45] D. L. Evans, P. Bond, and A. Bement, "FIPS pub 140-2: Security requirements for cryptographic modules," Federal Inf. Process. Standards Publication, Gaithersburg, MD, USA, Tech. Rep., 2002, vol. 12.

[46] R. E. Smith, "Trends in security product evaluations," *Inf. Syst. Secur.*, vol. 16, no. 4, pp. 203–216, Sep. 2007.

[47] Common Criteria. (Apr. 2017). *Common Criteria for Information Technology Security Evaluation—Part 2: Security Functional Requirements*. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[48] Common Criteria. (Apr. 2017). *Common Criteria for Information Technology Security Evaluation—Part 1: Introduction and General Model*. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[49] Common Criteria. (Apr. 2017). *Common Criteria for Information Technology Security Evaluation—Part 3: Security Assurance Components*. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf.

[50] H. Yajima, M. Murata, N. Kai, and T. Yamasato, "Consideration of present status and approach for the widespread of CC certification to a private field cases in Japan," Tech. Rep.

[51] K. Lee, Y. Lee, D. Won, and S. Kim, "Protection profile for secure E-voting systems," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.* Berlin, Germany: Springer, 2010, pp. 386–397.

[52] Australian Signals Directorate. (Jun. 2020). *Common Criteria Portal*. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/referral-organisations/common-criteria-portal

[53] Cyber Security Agency of Singapore. (Feb. 2021). *Cybersecurity Certification Guide*. [Online]. Available: https://www.csa.gov.sg/-/media/csa/documents/sccs/cybersecurity_certification_guide_v2.pdf

[54] M. Andrea, M. Philippe, D. Sbastien, and G. Jeremy, "Towards incremental safety and security requirements co-certification," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 79–84.

[55] K. Beznosov and P. Kruchten, "Towards agile security assurance," in *Proc. Workshop New Secur. Paradigms (NSPW)*, 2005, pp. 47–54.

[56] S. Xu, "The cybersecurity dynamics way of thinking and landscape," in *Proc. 7th ACM Workshop Moving Target Defense*, Nov. 2020, pp. 69–80.

[57] T. Benzel, "Cybersecurity research for the future," *Commun. ACM*, vol. 64, no. 1, pp. 26–28, Jan. 2021.

[58] Australian Signals Directorate. (Apr. 2021). *Essential Eight*. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/essential-eight

[59] Australian Signals Directorate. (Dec. 2021). *Assessing Security Vulnerabilities and Applying Patches*. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/assessing-security-vulnerabilities-and-applying-patches

[60] E. O'Connor. (Apr. 2008). *Patch Management Best Practices*. [Online]. Available: https://www.oracle.com/technical-resources/articles/it-infrastructure/patch-management-jsp.html#Reac

[61] F. Nicastro, *Security Patch Management*. Boca Raton, FL, USA: CRC Press, 2019.

[62] A. Sokri, "Cyber security risk modelling and assessment: A quantitative approach," in *Proc. 18th Eur. Conf. Cyber Warfare Secur. (ECCWS)*, 2019, p. 466.

[63] L. Liu, C. Chen, J. Zhang, O. De Vel, and Y. Xiang, "Insider threat identification using the simultaneous neural learning of multi-source logs," *IEEE Access*, vol. 7, pp. 183162–183176, 2019.

[64] S. Peisert, V. Welch, A. Adams, R. Bevier, M. Dopheide, R. LeDuc, P. Meunier, S. Schwab, and K. Stocks, "Open science cyber risk profile (OSCRP)," Open Sci. Cyber Risk Profile Work. Group Led by Trusted CI, Tech. Rep., 2017.

[65] S. A. Talesh, "Data breach, privacy, and cyber insurance: How insurance companies act as 'compliance managers' for businesses," *Law Social Inquiry*, vol. 43, no. 2, pp. 417–440, 2018.

[66] *BizCover: Compare Small Business Insurance Quotes Australia*. Accessed: Jan. 3, 2022. [Online]. Available: https://www.bizcover.com.au

[67] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4667–4679, Nov. 2016.

[68] MediaPRO. *2020 State of Privacy and Security Awareness Report*. Accessed: Jan. 3, 2022. [Online]. Available: https://www.bsigroup.com/globalassets/localfiles/en-ie/our-services/mediapro/2020_state_of_privacy-security_awareness_report_mediapro.pdf

[69] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, Oct. 2018.

[70] L. Zhang-Kennedy and S. Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–39, Jan. 2022.

[71] R. Sanders, "Embedding cybersecurity into your company's DNA," *People Strategy*, vol. 39, no. 1, pp. 8–10, 2016.

NAN SUN received the B.S. (Hons.) and Ph.D. degrees in information technology from Deakin University. She was a Postdoctoral Research Fellow at Deakin University. She is currently a Lecturer with the School of Engineering and Information Technology, University of New South Wales (UNSW), Canberra, Australia. Her current research interests include cybersecurity and social network security.

CHANG-TSUN LI (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from National Defense University (NDU), Taiwan, in 1987, the M.Sc. degree in computer science from the U.S. Naval Postgraduate School, USA, in 1992, and the Ph.D. degree in computer science from the University of Warwick, U.K., in 1998. He was an Associate Professor at the Department of Electrical Engineering, NDU, from 1998 to 2002, and a Visiting Professor at the Department of Computer Science, U.S. Naval Postgraduate School, in 2001. He was a Professor at the Department of Computer Science, University of Warwick, in January 2017, and a Professor at Charles Sturt University, Australia, from January 2017 to February 2019. He is currently a Professor with the School of Information Technology, Deakin University, Australia. His research interests include multimedia forensics and security, biometrics, data mining, machine learning, data analytics, computer vision, image processing, pattern recognition, bioinformatics, and content-based image retrieval. The outcomes of his multimedia forensics research have been translated into award-winning commercial products protected by a series of international patents and have been used by a number of police forces and courts of law around the world. He is currently the Chair of the IAPR Computational Forensics Technical Committee, an Associate Editor of IEEE Transactions on Circuits and Systems for Video Technology, EURASIP *Journal of Image and Video Processing* (JIVP), and IET *Biometrics*.

HIN CHAN is the Manager of the Australian Information Security Evaluation Program (AISEP) that resides within the Australian Cyber Security Centre (ACSC). The AISEP performs Common Criteria (CC) evaluation and certification of ICT security products for Australian Organizations use as well as to set standards to improve the security in ICT products. Within this role, he is the Australian Government Adviser on all matters related to product assurance and leads the strategic direction of Australia's International Common Criteria Effort. He is also an Australian representative at various international CC committees and ISO JTC1/SC27 working groups, and is a member of the Accreditation Advisory Committee (AAC) within the Australia's National Accreditation Body for testing laboratories, the National Association of Testing and Accreditation (NATA).

MD ZAHIDUL ISLAM is a Professor of computer science with the School of Computing, Mathematics, and Engineering, Charles Sturt University, Australia. His main research interests include data mining/machine learning, privacy preserving data mining, applications of data mining/machine learning in real life including cyber security.

MD RAFIQUL ISLAM (Senior Member, IEEE) is working as an Associate Professor with the School of Computing, Mathematics and Engineering, Charles Sturt University, Australia. His main research interests include cybersecurity, malware analysis and classification, security in the cloud, privacy in social media, and the dark web.

WARREN ARMSTRONG received the Ph.D. degree from Australian National University, in 2011. He is currently the Director of engineering at QuintessenceLabs, building cyber security products.