2023

Going beyond: Cyber security curriculum in Western Australian primary and secondary schools. Final Report

Nicola F. Johnson
Edith Cowan University

Ahmed Ibrahim
Edith Cowan University

Leslie Sikos
Edith Cowan University

Marnie McKee
Edith Cowan University

10.25958/41ZN-5R55
Johnson, N. F., Ibrahim, A., Sikos, L., & McKee, M. (2023). Going beyond: Cyber security curriculum in Western Australian primary and secondary schools. Final report. Report for the Cyber Security Cooperative Research Centre and the Office of Digital Government, WA.
https://doi.org/10.25958/41ZN-5R55

Going Beyond:

Cyber security curriculum in Western Australian primary and secondary schools

FINAL REPORT

Associate Professor Nicola Johnson
Security Research Institute & School of Education

Dr Ahmed Ibrahim; Dr Leslie Sikos
Security Research Institute & School of Science

Marnie McKee
School of Education

Cyber Security Cooperative Research Centre
Edith Cowan University

June 2023

Abbreviations

ACCE	Australian Council of Computers in Education
ACS	Australian Computer Society
ACARA	Australian Curriculum and Assessment Authority
ACSC	Australian Cyber Security Centre
ASC	Anglican Schools Commission (Inc.)
AISWA	Association of Independent Schools Western Australia
AITSL	Australian Institute of Teaching and School Leadership
ATAR	Australian Tertiary Admission Rank
ECAWA	Educational Computing Association of Western Australia
ECU	Edith Cowan University
F – 10	Foundation to Year 10
ICT	Information and Communications Technology
K – 10	Kindergarten to Year 10
MOOC	Massive Open Online Course
NAPLAN	National Assessment Program - Literacy and Numeracy
OECD	Organisation for Economic Cooperation and Development
PL	Professional Learning
P – 10	Pre-primary to Year 10
RRR	Regional, Rural and Remote
SCSA	School Curriculum and Standards Authority
SRI	Security Research Institute
WA	Western Australia/ Western Australian
WACE	Western Australian Certificate of Education

Executive Summary

There is no doubt cyber security is of national interest given the rife nature of cyber crime and the alarming increase of victims who have endured identify theft, fraud and scams. Curriculum within K-12 schools tends to be fixed and any modifications are subject to extensive consultation within a prolonged review cycle. Therefore, this report has gone beyond curriculum to explore the potential of national awareness campaigns and dynamic digital cyber security licences as alternative possibilities for instigation. The role of leaders in various school sectors and systems is critical for a successful roll out.

This final report culminates from a ten-month project involving the mapping of national (Australian) and Western Australian (WA) curriculum to identify cyber security content, knowledge, and skills, that is, where and if it is being taught. After the researchers released an interim report in late 2022, stakeholders were invited to read and respond to the report and its considerations. This final report includes a presentation of the findings collected during four stakeholder consultation workshops in December 2022.

In January 2023 additional consultation was made with the School Curriculum and Standard Authority (SCSA) of WA resulting in an enhanced and finessed interim report. This final report incorporates the bespoke WA context and historical developments of curriculum alongside detailing the extensive processes required for consultation and implementation. Furthermore, this report also features a preliminary literature review of international approaches to cyber security curriculum and the teaching thereof within K-12 schools. It points to different initiatives being taken up worldwide but also across Australia in a bid to educate young and future citizens about cyber-crime, cyber-risks and how to mitigate them, as well as indicating the importance of the security of the online environments within which education takes place. Given the rise of cyber-crime and the increased number of victims, and the interest and support for this research, it remains evident cyber security K-12 education is of national importance. The report surmises that the rate of change in cyberspace should challenge stable education systems, with teacher professional learning in cyber security helping to relevantly augment the current curriculum. Engaging in a national conversation about behavioural change can lead the way in addressing the high level of risk that individuals, including students and teachers, face online every day.

The report points out some considerations for immediate action:

- A national cyber security public health campaign targeting year 7 – 12 students.
- A national dynamic digital cyber security licence for students, teachers, and schools.
- Consultation with principals to identify professional learning needs of their staff.
- Teacher professional learning to develop knowledge of cyber awareness, cyber hygiene, cyber safety, and cyber security.

The work has been supported by the Cyber Security Cooperative Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

Table of Contents

List of Figures

List of Tables

Introduction

Overview of the entire project

This research project commenced in May 2022 and began with a goal to map the Australian national curriculum to identify where cyber security content was evident in the K-12 curriculum. This undertaking identified gaps, concerns, possibilities, and opportunities, and acknowledged limitations including that curriculum design is complex and curriculum is slow to change – due to many reasons. Version 9.0 of the Australian curriculum had just been released so that enabled a comparison of the previous version 8.4 to occur. We identified where cyber security concepts featured in the digital technologies learning area and in the digital literacy general capability (formerly titled information and communication technology general capability). The interim report also pointed to the cyber security focused content provided in the Year 11/12 Western Australian Certificate of Education (WACE)/ Australian Tertiary Admissions Rank (ATAR) subjects of *Computer Science* and *Applied Information Technology.*

Upon release of the interim report, an Edith Cowan University (ECU) press release stating 'Calls for five year old students to learn how to protect themselves online'[1] (31 Oct 2022) attracted extensive interest with subsequent web news items, radio and television interviews enabling 10 million individual views.

In the last week of November and first week of December 2022, four consultation stakeholder workshops were held. Participants from a range of diverse fields attended and they were invited as possible stakeholders. They were provided with the interim report and asked to provide feedback on the report during the workshops.

The School Curriculum and Standards Authority (SCSA) of Western Australia (WA) was also provided a copy of the interim report and the lead Chief Investigator met with SCSA representatives in mid-January 2023. Their feedback on the interim report was incorporated into the official published interim report (available at: *https://cybersecuritycrc.org.au/cybersecurity-curriculum-wa-primary-and-secondary-schools*) and informs this final report.

The main points of the interim report were:

- The Australian Cyber Security Centre (ACSC) identified 11 common cyber security threats for individuals and families. Five are not covered in version 9.0 of the Australian curriculum.
- The SCSA senior secondary subjects were up for consultation in 2022 and *Computer Science* includes a new unit on cyber security considerations. The Computer Science ATAR curriculum has finished the syllabus review process and is not proposed or in consultation. The finalised syllabuses are published on SCSA's website.
- Version 9.0 does include more specific cyber security language and has a new sub-strand *Privacy and data security* which focuses on protecting personal data through to systems analysis of cyber security threats.
- The teaching of cyber security skills and knowledge is highly dependent on the personal confidence and competence in cyber security of the individual teacher.

[1] *https://www.ecu.edu.au/newsroom/articles/research/calls-for-five-year-old-students-to-learn-how-to-protect-themselves-online*

Two provocative questions were included as follows:

1. Is it enough to teach school children to be aware of cyber security threats and to be able to protect themselves and their digital footprint through fundamental skills and knowledge such as multifaceted passwords and consider how they share information?

   Answer: The Australian Curriculum 9.0 will enable this.

2. Do we want Australian citizens to develop a deeper level of skills and understanding of the ways in which threats to cyber security might specifically cause harm in the ways that are outlined by ACSC?

   Answer: The Australian Curriculum 9.0 does not introduce the level required.

The WA curriculum published in the *Western Australian Curriculum and Assessment Outline*[2] sets out the mandatory teaching, assessing, and reporting on student achievement requirements for all Western Australian schools. In WA, Year 11 and 12 content is referred to as syllabus content for that subject, but in pre-primary to year 10 the content is referred to as the curriculum.

SCSA has completed a detailed audit of the endorsed Australian Curriculum version 9.0 against the current Western Australian curriculum. An extensive consultation process has occurred with teachers, industry professionals, universities, and system/sector representatives. SCSA then developed a Business Case for the WA State Government's consideration which documents the process for adopting and/or adapting the Australian Curriculum version 9.0 within the Western Australian curriculum.

In the second half of this project, we:

- Analysed the feedback from the consultation workshops.
- Commenced a systemic literature review of peer-reviewed literature.
- Incorporated grey and white literature surrounding cyber security initiatives within curriculum and schooling.
- Detailed various international approaches to cyber security in school curriculum.
- Identified the need to extend the scope of this project and extend the project with additional deliverables.
- Produced this report.

Literature review

Some international approaches to cyber security in K-12 school curriculum

In the Netherlands and the US, studies have found that the school curriculum 'hardly pays attention to cyber security', and the online behaviour of students is largely determined or influenced by experience, online instructions, and information obtained from family members rather than what is learned at school [1]. Teachers in the US are also calling for "proper" K-12 cyber-education [2]. Cyber security principles are currently being taught at the university level in computer-based courses, but rarely earlier, as is the case in South Africa [3].

In the US, outreach camps are organised for high school students, addressing online student behaviour and current cyber security issues. The need for cyber security training for K-12 staff has also been

[2] *https://k10outline.scsa.wa.edu.au/*

identified. There are arguments on teaching ethical hacking and debating whether it would draw students towards criminal acts [4].

There are attempts to integrate cyber security concepts in, or link them to, the existing curriculum, such as to introduce computer virus concepts in Biology lessons via making students understand how viruses spread, thereby drawing an analogy between cyber security and biology [5].

In Canada, the *Cybersecurity Classroom Training Program (CCTP)* features seven modules from Cisco's globally renowned Networking Academy, aiming to integrate cyber security concepts into core subjects, including Mathematics, Business, English, and Social Studies. It is the widest-reaching cyber security education program for high school students in the country [6].

The *K-12 Cyber Protection Framework (CPF)* also in Canada, aligns policy and a technological approach for K-12 schools to manage cyber security [7]. It aims at setting industry-led security and safety standards and guidelines, including privacy standards, for local school districts to deploy in K-12 schools. The Protection Framework has been designed specifically with education in mind, due to schools being targeted by malicious cyber activity because of only having low level security measures in place. The aim is having students understand, express, and manage cyber security risks, when their schools take on board the framework and policies. It allows schools to identify and prioritise actions that reduce cyber security risks and improve cyber safety across K-12 environments.

To address another reason why educational schools and organisations are being specifically targeted, a multilayered risk reduction model has been developed for high schools, tertiary and professional training in the Unites States [8]. Education is improving cyber defence activity and builds knowledge that confronts the criminal behaviour of adversaries. Whilst the framework requires ongoing adaptation as learning content changes, this industry-led development is reducing not only the institutional level risk but also that for individual learners, through a proactive approach.

Initiated by industry, the *New Brunswick Education Cyber Security Program* is a Canadian project-based learning content creator and pedagogy advisor program for K-12 classroom education that utilises curriculum guidance. The online program involves exposure to ethics, risk assessment, and data analysis across various courses, such as entrepreneurship, networking, and IT [9].

The *Cybersecurity 120 curriculum* is a teacher resource developed by Media Smarts, a Canadian not-for-profit centre for digital and media literacy. The program attempts to bridge the gap between key components in student learning based on requirements specified by post-secondary education and industry representatives [10]. The course is based on project-based learning, with learning outcomes targeting global competencies, operational skills, and computational thinking to analyse cyber-incidents and solve cybersecurity challenges via risk mitigation.

In Japan, the importance and appropriate use of authentication, along with not sharing passwords and not leaving laptops unsupervised, are taught in years 3 and 4 of primary school [11]. The learning objectives for years 5 and 6 are being able to use ICT that is not accessed illegally, understanding the reasons for not sharing passwords, and learning how to keep personal information from being leaked, as well as implementing measures to keep information secure. In lower secondary school (age 13-15), students acquire fundamental knowledge of information security, and learn how leaked private information can be used by adversaries.

The emerging pattern of approaches from abroad to learning and teaching cyber security are relying on and are being instigated by industry. Studies show frameworks are initiated by industry professionals to address either the present/future severe shortage of industry professionals and/or K-12 schools as high-risk targets to cyber threats. International studies purport that industry has been leading the way in supporting curricula in generating frameworks not only for within which cyber security training can operate securely, but also in the creation of learning resources for educators and learners.

Note that some country's initiatives in cyber security education are adapted not only locally, but also in other countries. A notable example is the ThinkUKnow internet safety programme, which has been trialled in Australia. While it has successfully improved students' knowledge on cyber-abuse, no consistent evidence of enhancing the students' risk perceptions or decreasing the likelihood of involvement in cyberbullying has been found [12].

Providing adequate cyber security skills and knowledge in schools from K-12 is a shared challenge among teachers and school administration. To address this, we can see combined efforts from the education community and industry have led to independent organisations being formed with specific goals. Some pertinent international examples are discussed first.

The K-12 Computer Science Framework[3] was developed in the US in 2016 with the aim to guide K-12 teachers teaching computer science. It outlines the core concepts students should know and practices students should exhibit essential to computer science. The framework can be used by a variety of audiences such as policy makers and administrators, curriculum developers, and computer science teachers. Topics related to privacy and security, and cyber security are addressed in specific areas of the framework or within cross-cutting practices. The framework is not meant to serve as a standard, instead as a guide to develop standard, curriculum, and teaching resources.

Figure 1 is an extract from the framework showing cyber security sub-concept, which is under the core concept of Networks and the Internet. The comparison between grades 3 and 5 shows that there are variations to the complexity of topics covered as well as crosscutting concepts depending on the grade level.

[3] *http://www.k12cs.org*

Figure 1: A comparison of cyber security sub-concepts covered for Grade 2 and Grade 5 for USA[4].

The Computer Science Teachers Association (CSTA)[5] on the other hand has published K-12 Computer Science (CS) Standards (in 2017) for teachers across USA and Canada by using the K-12 Computer Science Framework. The CSTA K-12 CS Standards provide a clear alignment with the CSTA Framework (Figure 2). The standard provides guidance to computer science teachers, schools, administrators, professional development providers, and policy makers. Furthermore, the various local chapters and virtual communities provide common spaces for teachers to provide and gain support from peers in their teaching.

[4] *http://www.k12cs.org*
[5] *https://csteachers.org*

Identifier	Grades	Standard	Concept	Subconcept	Practice(s)
1A-NI-04	K-2	**Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.** *Learning to protect one's device or information from unwanted use by others is an essential first step in learning about cybersecurity. Students are not required to use multiple strong passwords. They should appropriately use and protect the passwords they are required to use.* **Practice(s):** Communicating About Computing: 7.3	Networks & the Internet	Cybersecurity	Communicating

Figure 2: The CSTA K-12 computer science standards are aligned to the K-12 Computer Science Framework supporting teachers in the USA and Canada[5].

Emerging findings from a systematic literature review

We conducted a systematic literature review using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [13] framework. PRISMA is a widely used guideline to identify, select, appraise, and synthesise studies when reporting systematic literature reviews. The PRISMA statement was originally published in 2009 and later updated in 2020, which incorporates wider literature sources. Therefore, the current systematic literature review is comprised of academic literature as well as grey literature including but not limited to policies, frameworks, standards, and guidelines published by national and international government/non-government organisations.

The aim of the systematic literature review is to answer the following research question:

> *What approaches do other countries take towards cyber safety, wellness, and security for primary and secondary students?*

From a wide net of 2,500 relevant articles, the researchers identified 25 journal articles or conference papers significant to cyber security curriculum for primary and secondary schools. Most of these studies report specific research targeted at different levels of K-12 schools in different countries. Another commonality across the studies emphasises the development of resources from their country's existing curriculum frameworks to further develop resources supplementing teaching standards and quality.

While most of the studies were conducted in the USA, other countries include Canada, Netherlands, South Africa, South Korea, Turkey, Spain, and the UK. It is worth noting that "cyber security-specific" curriculum related articles from Asian countries were comparatively fewer in number than the rest of the world.

At this stage of the analysis, two emerging constructs we can identify from the data are 1) topic areas related to cyber security that are explored in the studies and 2) competencies that can be linked to students.

Topic areas could be classified within seven categories where aspects of Internet usage or students' presence on the Internet were most explored (30%) in the studies. This was closely followed by more general aspects of cyber security (22%). The complete breakdown of the categories is presented in Figure 3.

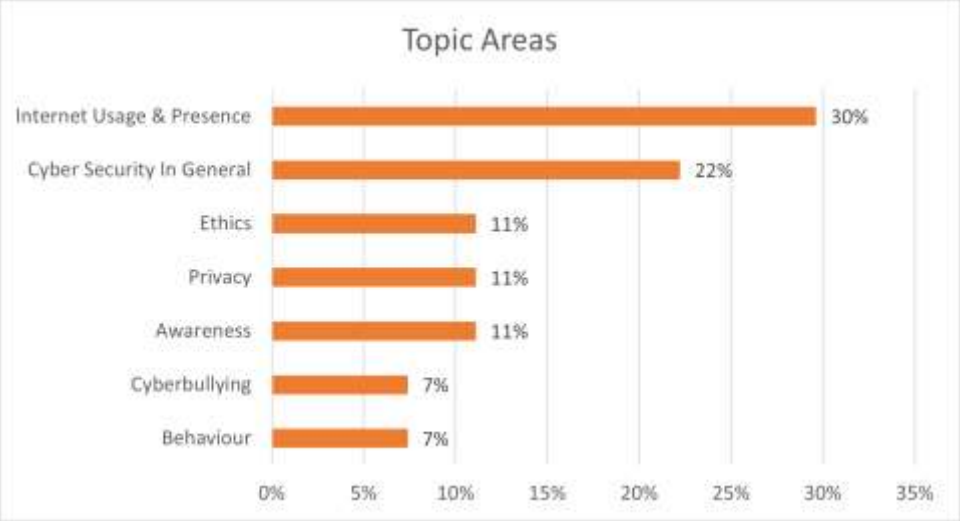

Figure 3: Seven categories of topic areas explored in the studies.

In several studies, students were tested for cyber security competencies. There are five areas of competencies we can see emerging from the analysis thus far. These include vigilance, social media and networking, online security, email security, password security. Competencies related to vigilance consists of more specialised skills (e.g., identifying risks or vulnerabilities) that cannot be generalised under the other four categories.

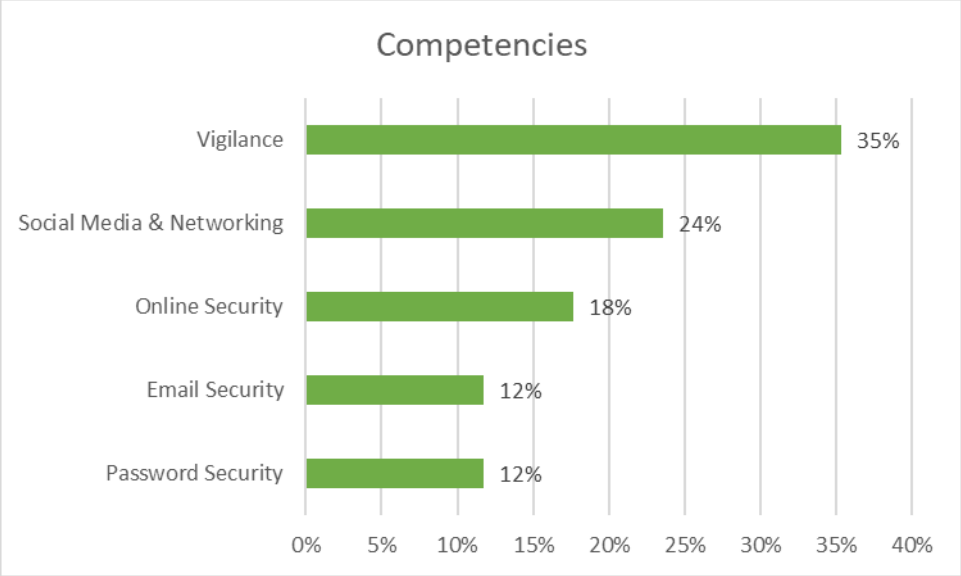

Figure 4: Five areas of cyber security competencies investigated in the literature.

Communities have been successful in assisting schools with learning standards for cyber content. For instance, in the US, the first voluntary K-12 cyber security learning standards have been released in 2021 by a national not-for-profit organisation, with the aim to contribute to the much-needed talent pipeline, thereby addressing the cyber security workforce shortage [14]. This was followed by the organisation's expansion of their Cyber.org's virtual lab environment, Cyber.org Range, available to teach cyber security skills to all K-12 students nationwide free of cost [15], having trained over 20,000 teachers in cyber security at the time of writing. The program touts to have increased student intake to cyber related college or university degree programs by four times as many students than high schools whose teachers have not received the training. This finding will be further explored in the extension of the project.

In South Africa, there are national initiatives such as the *South African Cyber Security Academic Alliance (SACSAA)*, established by three South African universities[6]. Resources are available for both students and teachers, including workbooks and posters. These are complemented by a range of activities, e.g., one-off workshops and talks by academia and industry intended to highlight the risks of cyberspace [16].

In Turkey, cyber security awareness surveys have been conducted in secondary schools. These surveys aimed at creating Internet security and computer usage awareness profiles of high school students. The surveys indicated insufficient student skills while testing competencies in terms of password security, online account security, social network security, and website analysis before software downloads [17].

In the UK, there are several national initiatives including, but not limited to, GetSafeOnline[7], Digital Wildfires[8], and Childnet[9]. For example, the latter released a poster and leaflet for 4–11 years old children on rules for safer Internet use[10]. Resources are available for both students and teachers, including workbooks and posters. In addition, activities like one-off workshops and talks by academia and industry are held, with the intention to highlight the risks of cyberspace. Two of the main issues identified in the literature are cyber-stalking and illegal trade.

The UK has also released a code of practice for online services entitled Age-Appropriate Design [11] that contains fifteen standards which any information society service likely to be accessed by children must follow. This statutory code of practice seeks to protect children within the digital world, not from the digital world. From September 2021, websites, games, social media platforms, apps, and streaming services were required to comply with these fifteen standards.

As we continue analysing both the academic and grey literature, we expect there would be more findings that will help us answer the research question tackled in the systematic literature review. The conclusion of the review will be published as a journal article.

Consultation workshop findings

Over one week from 28 November to 1 December 2022, the ECU's research team (the researchers) facilitated four consultation workshops of invited participant stakeholders to provide feedback on the project's interim report. Overall, attendants numbered 41. Three of the four workshops took place at Dumas House, hosted by the Office of Digital Government, and one took place as an online meeting. The initial email invitation read as such:

---

6 *https://www.cyberaware.co.za*
7 *https://www.getsafeonline.org*
8 *http://digitalwildfire.org*
9 *https://www.childnet.com*
10 *https://www.childnet.com/resources/be-smart-online/*
11 *https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/*

Thank you for your interest in attending one of our upcoming cyber curriculum stakeholder consultation workshops.

Here is the link [12] *to a 4 ½ minute introductory video on YouTube providing the context and introduction to the interim report and the workshops.*

Please ensure to thoroughly read and engage with the attached Interim Report entitled, ***'Cyber security curriculum in Western Australian primary and secondary schools'****.*

Please come to the workshop having read the report and reflected on your responses to the following questions:

a. *What do we need to do to ensure curriculum, schools, teachers, and students are agile to respond to fast-moving, ever increasing cyber-crime and threats?*
b. *Regarding the report, what are your queries and concerns, clarification questions, and suggestions for consideration?*

We look forward to seeing you there and invite your active participation in the workshop.

Each workshop comprised a heterogeneous group of participants from across educational, computer science and cyber security sectors. Attendees included early childhood, primary, secondary, and tertiary educators, and principals. Representatives from information and computer technology (ICT) specialist schools, educational organisations, and both new and established companies across the cyber security and related industries attended. Most of the professionals attending had cross-sector experience: ex-teachers now working within cyber security or higher education; ICT specialists moving into schools and student-age extracurricular learning program service providers; and managers/facilitators within specialist digital/science education organisations. Also represented were people with interests in regional and remote WA including distance education, the needs of students in isolation, as well as students in hospitals, early childhood centres, and home schooling.

As a forum for industry and education coming together, the workshops provided a definitive measure of enthusiasm across the board for cyber security to have a stronger focus within WA primary and secondary schools. The atmosphere was more than congenial across the four workshops, often electric with excitement for the breadth of potential the subject could bring to both industry and learning spaces, *and* in feeding into the national conversation on public health in this country. Rich and deep discussions took place led at times from stakeholder workshop attendees, then also by the workshop leaders (the researchers, named above) with specific questions, leading to the realisation of the openness on all sides for a deeply collaborative approach to not only the development but the structure to WA's education of cyber security.

Overall response to the interim report and its context

The support received for the report was overwhelmingly positive with media coverage across the Asia-Pacific region reaching 10 million views in November 2022. The cultural backdrop for the workshops held November and December 2022 included the personal data breaches via Optus in September and Medibank in October that year, both events widely presented in news media as leaving ~9.8 million Australians with compromised identities, as stated by the Department Home Affairs. The report's timely release coincides with a pivotal moment in Australia's technological history, highlighting the urgency for action in the education sector regarding this important subject that demands attention on a broad scale.

[12] *https://youtu.be/vWE2su77UgE*

Attendees agreed that bringing cyber security into the WA curriculum is a huge undertaking but a necessary one because leaders within industry and education want to build a secure state of digital citizens in this digital age. The economic need to build a skilled cyber workforce is definite, yet we do not have required resources systematically distributed through schools. The shorter-term threat of cyberattacks grows exponentially upon us, and whilst cyber security is being addressed at the national level, for instance via the recent appointment of Australia's first Cabinet Minister for Cyber Security and an Expert Advisory Board, it is in its infancy. At the time of writing a Discussion Paper was released by the Department of Home Affairs calling for submissions to feed into a national conversation on the 2023 – 2030 Australian Cyber Security Strategy [18] with the aim to "make Australia the most cyber secure nation in the world", as stated by The Hon Clare O'Neil MP in the Foreword.

The Workshop Findings of this report suggest that to further strengthen a technologically skilled workforce through education, there is potential via industry collaboration and project-based learning. Providing teacher professional learning to enable relevant curriculum to be augmented needs to be coupled with a collaborative approach with industry. Because we do not have the workforce we need, but we do have rapidly increasing threats surmounting daily, we must move fast to enact change. Augmenting the curriculum is one reinforcement for generating that workforce but on its own, is not going to resolve the issues we already face.

Cyber security is pervasive, and so it should be considered and discussed across all learning areas where relevant rather than be established as its own new learning area. Children need to be cyber aware in the learning environments provided for them at younger ages. Attendees agreed that cyber safety is not enough. Students must learn secure online behaviours and the ethics surrounding our choices in cyber space as early as is relevant to online exposure. The consensus from stakeholders is to teach children early the hygiene, the dangers, and that our digital footprints last forever. By year 8, based on their interest and positive experiences with Digital Technologies, students decide whether to take Digital Technologies (it is only an elective unit) in year 9 and above. This means so many students miss out on the only learning area to specifically focus on high levels of essential cyber security content and skills (especially at senior secondary Computer Science levels).

Workshop attendees agreed that teachers should not be the ones shouldering this responsibility. Because we are talking about risk and mitigating risks, school leaders are key to the incorporation cyber awareness, cyber hygiene, cyber safety, and cyber security within schools. Hence a top-down approach whereby governments lead the change via school leadership and teacher professional learning enables an augmented curriculum to feed into a workforce that comprehends the value of cyber security. However, one must consider the relational and contextual sites within which teachers are learning and practicing and support them to address cyber security as a significant issue as teachers have an extensive role in building generations of savvy computer users.

A national digital cyber security licence

Mentioned by multiple attendees in different workshops was the recommendation for a digital cyber security licence for students, teachers, and schools. This licence would be like a swimming certificate in that it is developmental and commences with cyber awareness, then incorporates fundamentals of cyber hygiene (best practices), followed by cyber safety and higher levels of cyber security. Due to the need for swimming and the expectation that it be taught in schools, despite not being part of the curriculum, there is buy-in from schools to provide swimming lessons (for a fee) and include a certification sign-off summative process. The courses and its taught content are independently provided by the separate entity Swim Coaches and Teachers Australia. It is proposed that an extension of this project designs a developmental digital cyber security licence for school students over three stages for primary, which can be continued into secondary school with additional stages of achievement. In addition, a digital cyber security licence for teachers would be developed to reflect developmental knowledge and competencies of which professional learning would help increasingly difficult stages to

be met. Finally, a digital cyber security licence for schools would be created to help support schools to implement cyber secure and cyber hygienic best practices from a basic to an advanced stage. The ECU research team would design the licences, seek feedback, and then roll-out the initiative with support from government agencies and departments as required.

An incessant need for understanding and change

There are many very different components to the digital arena of which cyber security is merely one. Though its nature is ubiquitous, the impact on us all falls at the cultural and individual levels, as well as the economic. Not only are there broad misunderstandings amongst most communities as to what cyber security is and the interplay with other related but equally important cyber concepts, there is a realisation required in the public realm that we as a state (and country) need to understand that we must, every one of us, change our behaviour when it comes to securing our devices, identities, companies, and industries.

The current situation, echoed workshop attendees, is a national health crisis, due to a lack of public knowledge about the importance of cyber security today. The role of the school curriculum in addressing cyber security is part of the solution but is towered by the present risks and potential disruption to ongoing operations of not only schools, but all personal and business activity involving digital devices and online interactions. In the past, an efficient way Australia has changed its behaviour has been through national awareness campaigns.

A public health campaign from a nationally aligned voice of authority

Stakeholder participants advocated for three key behaviours needing to be encouraged from the top down:

1. using a password manager;
2. using multifactor authentication; and
3. updating devices.

The responsibility to address students' learning of password security protocols to protect identities against fraud, as well as keeping schools' online activity secure are the tip of the iceberg. Workshop attendees stated that we cannot stop there, as people's and businesses' actions demonstrate every day the common misconceptions of what cyber security is and who needs it. When talking about cyber security, one also needs to address the related concerns of cyber hygiene and cyber safety, as the terms are often used interchangeably. Therefore, the learning required "must start from a universal understanding, operating from a set reference point", a stakeholder stated. We need a stable lexicon from which to build a shared understanding across all facets of our society in using devices online.

Stakeholders believe we must start with an awareness campaign reaching all our communities, as the risks increase around the protection of business brands, finances and production, the protection of machinery and infrastructure, sensitive information, and documentation; the economy and everyday life as we know it. Without a systematic societal-wide approach the threats to our economy and wellbeing remain at the current high level. Hence, we "hands down cannot leave it up to teachers," said one attendee, "because the pervasive skillset needed across all industries and all workers to keep our identities and workplaces secure, requires a whole system initiative". That system is much greater than schools.

A whole system initiative, said stakeholders collectively, is the approach necessary for the level of change required in the immediate timeframe. Whilst cyber security and its associated sectors are very self-organised nationally, they do not have the networks, know-how or time to engage people at this level, said stakeholders. They argued that it is state bodies which need to lead a fundamentally

collaborative effort across industry and education sectors, with the support of state if not national budgets.

Workshop attendees together spoke through the idea of a state campaign, raising examples to emulate that have been successful in changing the behaviour of a nation. The awareness campaigns brought up by stakeholders were Cancer Council's Slip Slop Slap to protect ourselves against skin cancer launched in 1981, the WorkSafe WA campaign of the mid 1990's, and the preeminent longstanding Constable Care movement for road safety in WA. Industry and educators are calling for a national awareness campaign not unlike Slip Slop Slap to protect ourselves from cyber criminals.

One stakeholder's opinion was echoed: "The concept to me is how to facilitate that Slip Slop Slap type campaign in a cyber sense so that it's not daunting for teachers to take on" then that language becomes part of the conversation with teachers and "part of the common vernacular across communities through a widely supported public awareness campaign". Any such campaign would be aiming to achieve a long-lasting effect through the consistency of the message. This could be through a program or the campaign itself for instance, as a "broad banded strategy", the researchers heard.

To springboard a campaign, the suggestion was made to embed a broader cultural understanding of the need for cyber security and how it effects all of us, through a launchpad event equated to Indigenous Learning Week, perhaps aligning with the recently launched National Password Day on 4th May. Such a springboard milestone would do well to be presented by authority organisations and hosted by current public figures.

SECTION SUMMARY

The timing of the report's workshops aligned with the nation-wide breaches of users' identities in late 2022. Whilst extending the presence of cyber security into the Australian Curriculum 9.0 is a mammoth task it is necessary to build a state of digital citizens in a digital age. We are not resourced nor organised for the changes already upon us, that is, to fulfil the need for a skilled cyber workforce, nor implement the curriculum change fast enough to address the exponential growth of cyberattacks.

To build a tech savvy workforce Australia needs a collaborative approach with industry and educators. Industry professionals will need to feed into school learning through project-based (or inquiry-led) learning approaches and in so doing improve their soft skills. But curriculum-based education alone is not going to resolve the issues we already face.

Cyber security needs to be addressed in the curriculum across learning areas as well as starting much younger than is currently outlined, inclusive of grounding learning in ethics, psychology and understanding ethical and criminal behaviours. Cyber-safety is not enough. We also need to overcome the current issue that Digital Technologies is only an elective unit from year 9 onwards, and so many students are missing out on important content that is relevant to all.

Whilst school leadership is where responsibility falls for security in schools, to keep our workplaces and identities secure, a top-down approach is required whereby governments lead the change, principals support the initiative, teachers are provided with professional learning so they can best augment the curriculum to produce citizens who feed into a workforce that comprehends the value of cyber security. Cyber security is misunderstood by society and the terminology is unclear. This current situation is a national health crisis and nation-wide behavioural change is required. This towers the role any curriculum role can fulfil.

Stakeholders propose a national awareness campaign from a nationally aligned voice of authority, similar to the Slip Slop Slap campaign. Such a campaign purports an approach necessary for the level of change required in the timeframe it is required in. This approach regulates the lexicon and becomes part of the national conversation, trickling down to that with teachers as a broad banded strategy. To

springboard a campaign, a launchpad event equated to Indigenous Learning Week presented by authority organisations and public figures might assist. The three key behaviours to be encouraged are: 1) using a password manager; 2) using multifactor authentication; and 3) updating devices. Furthermore, state bodies need to be leading collaborative efforts across industry and education sectors, with the support of state if not national budgets.

The current and future position of schools and the curriculum

Schools falling behind community and industry-led training

Due to the fast-paced nature of changes in cyber, schools are now necessitating 'playing catch up' to regain traction and meet the broader community's needs. The researchers heard of the current trend of industry moving on with education, with or without schools. International companies are partnering directly with small community organisations and government agencies, as well as training school-aged children to provide cyber secure educational initiatives. For instance, one free online Saturday morning workshop in cyber training received 1,500 registrations, stated a tech giant workshop attendee.

Addressing cyber security in schools enables schools to recoup relevance before being left further behind or valued less by society at large, as measured by students leaving early to find relevant private training, or industry 'snapping up' students with extracurricular training over curriculum-based pathways. The researchers heard the extent of the trend of students and industry preferring micro-credentials, bypassing school curriculum, and being accepted into university. Such student pathways are closer to meeting the real life needs of industry and remain relevant not only because the learning content changes with the times, but because the learning environments young people are exposed to increase their transferable skills of collaboration, problem-solving and communication.

As students become the workforce of the future, we are readying young people to engage and lead industry through unsecure times. But with cyber security issues moving so fast, a burning question arises, how do we ensure learning content does not become redundant even when changes to the curriculum *are* made?

Wider industry support available for schools and teachers

An overwhelming number of companies and organisations attending the workshops made generous offers to be part of the build and implementation processes. With such an eagerness for cross-sector collaboration being emphasised by stakeholders, it appears schools and teachers could be well supported through cross-sector industry/educational collaboration. Individuals are keen to invest their time ensuring teachers, principals and schools are duly supported. Such an integrated and collaborative approach to implementing cyber security assists everybody. The workshop conversations reinforced that substantial changes to curriculum could only occur within an environment of significant and equally broad government-led resources, supported by a public awareness campaign to support community cyber awareness.

Working towards an augmented curriculum

Some of the teacher participants mentioned and supported the idea of augmenting the curriculum with aspects of cyber hygiene, cyber safety, cyber awareness, and cyber security. Instead of changing the curriculum or adding to it (meaning some things would need removing), provide professional learning for teachers so they can highlight and point out implications for all things cyber as they go about teaching the curriculum. One stakeholder mentioned using the 'teachable moments' to reinforce cyber safety practices. Given the prevalence of digital device use and the incessant spamming and scamming that occurs, incorporating a focus on or reminding about 'all things cyber' throughout the school day appears

workable. One participant emphasised context and 'real-life' issues, hence there is an opportunity for teachers to incorporate cyber security awareness through the teaching of the eight learning areas (where relevant).

Project based learning environments are key

With the curriculum being augmented to include ongoing industry input, we have an opportunity to further create 21st century thinkers and doers, via an integrated approach to project-based learning. That is, stakeholders explained, students (and teachers) work together in schools with industry professionals within collaborative learning environments that are situational or context-led projects. These are also known as or very similar to inquiry-led projects (Department of Education NSW uses this term within their approach to their year 9 and 10 cyber security elective unit, see below for more about this). There are countless opportunities to keep project content relevant to students' interests. In this way we build on students' interest and highlight technology-led career paths.

Project environments can immerse students in a problem-solving process without students particularly realising they are engaging in or *doing* learning. In project-based learning environments, students improve their soft skills through interpersonal negotiation, which mimics cyber industry working environments, utilising skillsets directly relevant to industry needs, for instance in practicing "incident response" skillsets and capacity building. An example offered of a classroom project starting point was role-play based, "You are a CEO, what do you do?"

Whole school learning approach

Whilst teacher professional development remains a critical component to implementation, it is suggested any teacher education rollout should be delivered to whole schools and not individual teachers, as responsibility must be understood at the cultural level of a school. By acknowledging and addressing the context within which teachers operate we reinforce the value of not only the teachers' extensive role within the changes required ahead but the fundamental learning environment within which secure behaviours are to be established.

The researchers heard from workshop attendees of a successful model being used within industry via a trickledown effect. This model is interpreted like a project, whereby schools are being audited on their own cyber security hygiene practices. The learning by school leadership from the administrative project trickles down to teachers then students, and then out to families and whole school communities. Such an approach maintains accountability of online (safety and) security with school principals (as well as in some educational sectors board directors, for instance, in independent schools), as they are in the positions in charge of risk.

Leaders to be leading

A popular standpoint amongst stakeholders was echoed by an educator in saying, "I see (the responsibility for cyber security) as distinctly a principal's role. I see that role as being the enabler. Also to be appointed is a lead teacher to manage the implementation, (whilst the leadership) provides conditions within which they are able to implement". Furthermore, if school leadership were to be mandated to complete cyber awareness and security training, "we send a powerful message impacting the school community's psychology as to the subjects' importance", said another workshop attendee. Strengthening earlier comments, they said, "someone needs to be nominated as the risk holder. Whoever that is, they are the ones who need the training."

Reinforcing the project-based modelling approach ensues when we capitalise on ICT industry knowhow as the leaders in their fields and bring them into schools (and not the other way around, said attendees). Leaders enter schools to guide audits and notionally 'stay' and continue to mentor/guide the school's framework for integrating cyber into teaching.

Shift the mentality of a generation

As mentioned, stakeholders argued the level of change required exists well beyond the whole school level. “How do we teach these principles if we are not living them?”, asked one industry stakeholder. “Why would we only consider schools as organisations being responsible for their cyber security, and then not also be addressing all other companies’ leadership being responsible for their cyber security in a similar manner?” The workshop conversations spoke to a level of culture change being asked of us as a society.

Researchers heard private organisations are not taking cyber security seriously unless they are being forced to by their security providers, which is increasingly being required to receive services. For instance, a Perth networks and security provider to local government has (as of April 2023) mandated certain protocols to *existing* clients, “or they walk”.

Whilst reporting for finance and occupational safety is required, and training in child protection training is obligatory for board directors, cyber security is currently excluded from such legal requirements. Examples given by workshop participants included whole hospitals’ staff not having secure passwords and universities not enforcing training protecting against risks such as opening emails from outside of the organisation. It was discussed that many local governments are being audited and are matching state government, but broader change needs to be instigated by mandating security levels in business to embed the knowledge into the cultural fabric of society. “Incentivise or mandate it”, said one attendee receiving resounding acknowledgment.

Big stick approach

In coming from the top-down where governments lead whole schools, and across the whole of the state, a ‘big stick approach’ (that is, asking nicely whilst holding a stick) shifts the mentality of a generation. Australians’ response to the Covid-19 pandemic demonstrated that when individuals understand what is at stake and what is required to keep their schools, workplaces, and livelihoods secure, we change our behaviour to safeguard our way of life … and we can act quickly.

With the backing of the incredulous national shift in mindset due to past successful awareness campaigns of Slip Slop Slap and others, and because of the pandemic, stakeholders were matter of fact in stating a public health campaign is a “no-brainer”.

SECTION SUMMARY

Schools are falling behind community and industry-led training with students leaving early for relevant private training and industry ‘snapping up’ students via extracurricular training. Addressing cyber security in schools enables schools to recoup relevance before being left further behind. With cyber security issues moving so fast, how do we ensure learning content does not become redundant? Wider industry support is available for schools and teachers. Stakeholders wish to collaborate across industry and educators to develop teacher professional learning. The answer lies in providing bespoke teacher professional learning of all things cyber, alongside a public awareness campaign to support community cyber awareness.

There is an opportunity for teachers to incorporate cyber awareness, cyber hygiene, cyber safety, and cyber security augmenting the teaching of the eight learning areas. When learning cyber is addressed at the cultural level of society and the whole school, teachers are supported. If school leaders are required to embed cyber secure practices within schools, teachers will also be supported. This trickle-down effect will help to shape the cultural fabric of society. Incentivise or mandate it.

The task at hand is bigger than curriculum implementation

Shortage of teachers, shortage of tech industry professionals

There has been a lot of media exposing the overwhelming realities teachers face, noting the burnout and exodus from the sector. Teachers are in high demand and are being accepted into teaching positions prior to completing their qualifications (as pre-service teachers). Reminding us of the imperative nature of bringing cyber awareness into schools was a scenario explained during a workshop. A stakeholder shared an anecdote where a training college recently ran a series of cyber skills workshops designed for teachers to help build the teacher workforce, but in the process recruited five of those teachers to their own organisation!

A cultural shift is required

There was considerable agreement across the workshops to not burden teachers anymore, particularly because the immediacy of the threat following the Medibank and Optus data breaches of 2022 identified the breadth of our cultural comprehension of cyber security, or lack thereof. These incidents of threats to identity across the nation set the tone for each workshop that people's comprehension of cyber security is a problem much greater than individual teachers and their professional development can impact and falls even beyond the reach of schools'.

The researchers heard from a stakeholder that in comparing a level 3 school in the wheatbelt to an 1800+ student school in the city is reason alone as to why the responsibility of cyber security does not fall onto schools, at least not yet. They continued, "Change needs to come from administration. It needs to be supported from the top down – and then down into the classroom. It is not up to those who are not providing the planning for cyber security, these are people who don't have the skills or see it as a priority". Other comments included, "We need an awareness across the whole community for this to be effective"; and "If we leave it up to schools, there is a limit to funding and staffing and the learning will be presented within that limited context. But this is a national crisis". While the issue of access and equity needs attention, alongside the increasing divide between schools that 'have' and schools that 'have not', another is the inconsistent messaging ranging from the current failing approach of protectionism. Hence any messaging needs to align across and reach all (Western) Australian communities, schools, and homes.

One stakeholder's view pointed to the idea that people think cyber security is too technical or too dry and are overwhelmed by it. There is an associated mythical image requiring dispelling that cyber security is a "person in a hoodie in a dark room with a computer." They continued, "We need a cultural shift before cyber security makes it into the curriculum so that it becomes a belief as to its importance, in protecting our data and our identities".

Call for a national awareness campaign for a public health crisis

To springboard a campaign, the suggestion was made to embed a broader cultural understanding of the need for cyber security and how it effects all of us, through a launchpad event equated to Indigenous Learning Week. Such a springboard milestone would do well to be presented by authority organisations and hosted by current public figures. Such a campaign would have a two-pronged approach of informing the public alongside its implementation in schools.

SECTION SUMMARY

There is a shortage of teachers and a shortage of tech industry professionals. Teachers are at risk of burnout, and we cannot burden teachers anymore. The recent national incidents of identity theft reinforced that schools cannot resolve cyber security issues alone, and if we try, any cyber learning will be presented within the context of limited funding and staffing. This is a national crisis falling beyond school jurisdiction at the outset. The work completed for this report has led us to consider going beyond the curriculum to explore the potential of employing other strategies to address these issues – see the 'considerations and recommended actions' section.

What the cyber industry needs – soft skills, not technical, please!

Surprisingly it is students' soft skills (or transferable skills) that the information and computer technology (ICT) industries and the tertiary sector are looking for in school leavers, above and beyond technical knowledge.

Soft skills not technical, please!

Having been the forerunners in dealing with cyber security on their own in Australia, the cyber security industry has become very organised, consistently holding national conversations. The researchers heard from many workshop attendees how only weeks prior this report's workshops the conference attendees from a national cyber security conference held in Perth (November 2022) identified the skills most valued and required to enter the technology sector, *as a conference-wide exercise*. Again, the skills are not technical but are in fact the transferrable skills of: problem solving; collaborative skills; ability to communicate; and to demonstrate initiative. As mentioned, these industry conclusions were reinforced by many other report stakeholders, including a WA ICT specialist school principal in saying that within their school, the learning of technical skills was near impossible without this foundational soft skillset.

This sentiment was reinforced within another workshop where a schoolteacher commented on the teaching of digital ethics that:

> *At the moment, workplaces are grabbing students straight from school who can communicate effectively, rather than those who already have the technical skills. It is the ethical side, ability to analyse and problem solve that are the students being called for in industry. And we can incorporate digital ethics (in the classroom learning) across subject areas.*

Another aspect raised was the need to gain further understanding of the standards tertiary institutions are looking for in terms across both knowledge and soft skills. It should be noted many soft skills are included in the learning areas (especially English, Humanities and Social Sciences, Science and Health and Physical Education), but are not necessarily listed under a cyber security heading. It was noted that no WA university offers a major in digital technologies initial teacher education secondary programs.

…and an understanding of digital ethics

Understanding digital ethics was an ongoing subtext within workshop conversations and became synonymous with the idea of positive online behaviour - a clear crossover between the workshops' cyber safety conversations and that of cyber security. Both spaces denote a level of awareness and care for others and for oneself. One attendee stated, "ethics needs to feature in teaching (positive) online behaviour, and this content can be easily gamified." It should be noted 'ethical understanding' is one of the general capabilities of the Australian curriculum and includes the organising elements of 'exploring values, rights and responsibilities', 'reasoning in decision-making and actions' and

'understanding ethical concepts and issues'. In version 9.0 of the Australian curriculum, Humanities and Social Sciences is tagged with the highest proportion of content descriptions regarding Ethical Understanding. This is followed by Technologies then Health and Physical Education. These three learning areas do include a focus on interpreting, analysing sources of information and decision-making which arguably comprises aspects of cyber safety and security. As stated in the interim report, these capabilities complement curriculum content but are not assessed in Western Australian schools.

Tech industry professionals want to collaborate with schools

If Australian curriculum developers take on board what industry is asking for to overcome the lack of skilled workers within cyber, the approach to school student learning would allow children to practice their soft skills whilst gaining understanding through experiential 'enquiry' into current cyber security, hygiene, and awareness topics. This approach directly mirrors standard industry practice and is seen as a necessary approach for success to incremental change, said workshop participants. Industry people can offer up-to-date experiences where students learn the tradecraft of identifying threats and vulnerabilities. One participant explained, "the idea of having educational structures as stable is fundamentally incompatible with cyber. Everything will be different in two years' time". Currently the Australian Curriculum, Assessment and Reporting Authority (ACARA) who are responsible for the national curriculum, review curriculum subjects over a six-year cycle.

We cannot have the expectation that teachers have technical knowledge, said a school principal within a workshop. They continued by saying,

> *… industry are putting their hand up offering to teachers and students to come in and talk with us and create ongoing relationships with us. Having open ongoing conversations allow us to help schools know what is relevant for students as well as the other way around. For instance, by knowing the applications students are currently using, we as educators can prevent the outcomes from predatory behaviour. Currently it is TikTok where users are particularly vulnerable, but this will change. Additionally, the cross-sector integration make for very engaging experiences for students, which activates their interest in the subject areas. This approach will build student numbers into choosing technical elective units.*

Through partnering with industry, schools can explore the potential of industry-led projects-based models to help address the need for filling jobs within cyber.

Where schools and industry are already collaborating

Some collaborations have been established between industry and schools. Schools and government are themselves independently leading the way in research and implementation, to overcome the skills shortage in industry and address behavioural change to remain cyber secure. Many teachers and whole schools with the resources are applying what they know, some becoming a 'tech school' through Education Department's Approved Specialist Programs within the ICT stream of WA specialty schools. A workshop attendee provided an example from one such school receiving funding for an industry liaison at their school acting as a mentor.

As an example of how collaboration with industry is already working within schools, according to that tech school's principal, they received overwhelming interest from tech companies to partner with their school. The result of their approach to include industry in student learning has skyrocketed into the school's involvement with industry-based international events, being asked to share their approach of what it looks like to be immersed within industry. This then resulted in a further thinking forum within the school community. The school asked the community, 'what is the most important aspect we need to implement?' Now the school has a 'cyber security solutions' program. The school had successfully engaged its community to build and implement the changes required.

Furthermore, the tech school has also been able to feed back their findings to industry, at a 'high level', as acknowledged by other industry stakeholders who had seen that school's students presenting their projects, describing the high school students as operating at tertiary level. Other schools in the state of Victoria were also named as running on similar models, with one high school partnering with a university and local TAFE.

Other state and national bodies are also very active in the collaborative space. A representative from ACARA attending the workshops reminded us that they as the national authority on the curriculum have already presented to the integration of the Digital Technologies units within the other learning areas. Genuine connections have been made across maths, health, and physical education. Teachers will find other opportunities and links, the representative mentioned.

In November 2022, the WA Premier sent out a circulatory mandating that all government entities report cyber incidents to the WA Government Cyber Security Incident Reporting Portal because, says the policy document, "Government is dependent on reliable and secure digital systems to provide public services." The follow-on here is that government schools also require secure and reliable digital systems to provide the public service of schooling. This reinforces this report's position, which reflects the stakeholders' position, that of the trickle-down approach of securing schools' digital systems, then addressing the curriculum via a flow-on approach with professional learning and bringing cyber industry professionals into schools.

Whilst key organisations and governments are active in addressing the cyber issues at hand, a more coordinated, wholistic response is being called for that includes enveloping the general public and industry across all sectors, across all of the state (or country).

SECTION SUMMARY

The progression of cyber learning over schooling stages has been addressed with broad brushstrokes within the report. Aspects of cyber security need to be taught early on to mitigate risk and to encourage ongoing early interest.

Industry and the tertiary sector are looking for soft skills in school leavers, above and beyond the more expected arena of technical knowledge. Those transferrable skills have been named as: problem solving; teams and collaborative skills; ability to communicate; and using initiative. Workplaces are grabbing students straight from school who can communicate effectively and understand ethics, rather than those who already have the technical skills. Digital ethics must be incorporated into classroom learning across learning areas. Further understanding is required of the standards tertiary institutions are looking for. No WA university offers a major in digital technologies initial teacher education.

The idea of having educational structures as stable is fundamentally incompatible with cyber. But tech industry professionals want to help educate in schools to lead the charge, with cross-sector integration making for very engaging experiences for students, activating student interest toward choosing technical elective units in middle upper school.

A more coordinated, wholistic response is being called for that includes enveloping the general public and industry across all sectors, across all of the state (or country), now that broad collaborations have been established between some schools, industry and tertiary, and are leading the way in research and implementation.

The WA Premier recently mandated all government entities report cyber incidents. The follow-on is that Government mandates security responsibility, accomplished by means of schools taking on a trickledown approach of securing schools' digital systems, addressing curriculum change via a flow-on approach with professional learning, and bringing cyber industry professionals into schools, with a whole school schema.

Barriers to change

Stakeholders' bigger picture in the education space

The realities schools face on the ground also require attention to effectively augment the curriculum and play a part in the changes ahead. Because the different educational jurisdictions across public, independent, Catholic, and other school types are tackling challenges differently, the overarching coordinated response stakeholders are calling for needs to originate from above those jurisdictions, that is, government. Note that some of the barriers described below may or may not relate only to public schools but are addressed here generally.

Online concerns: equity of access

Across WA, it appears students do not have equitable access to working digital devices, resources, and technicians. Workshop participants agree that "we are receiving no specialist staff in primary schools, and are paying out for specialist technicians for any software issues. And that costs. If it is a regional / remote school, it is almost impossible in most instances (to supply and maintain computer access securely)." Participants considered access and maintenance of hardware an insurmountable issue unless the state steps in to generate a system whereby digital devices and technicians are accessible on an ongoing capacity.

Understanding privacy protocols

An instance explained in a workshop regarded the need to maintain a level of privacy when online, as we do in the real world. In many schools when using laptops or tablets, the teacher provides the school's online account and everyone shares the passwords. This is to facilitate ease of use and log on. Students finish the lesson, then simply close the lid, or even leave the computer open and vulnerable. It is worth noting is that sharing passwords is against Department of Education's policy.

To overcome that issue an industry attendee explained, "we entered (the) school, teaching students the first steps of logging out, and emphasising its importance. Then we introduced a secure remote access desktop space, and the desktop kicked them off (towards secure practices). Even for the adults, it became fun because the experience was gamified, and people adhered to the protocols after that."

eSafety

The behaviour of children (and us all) while we are online is not yet being addressed well. The negative psychological, neurological, and physical impacts happening to us all individually while we are online is not widely understood, nor being discussed within communities who have not had training from industry professionals. This situation speaks to online safety as a key area to be addressed.

The psychological effects of cyber space on our young need to be known publicly already, as part of the government public health message, say stakeholders. Anxiety and stress in our children is increasing. An example given was the number of extensions being given out for school students' work completion on the grounds of recognised anxiety.

Broader factors to consider toward curriculum inclusion and public awareness

Some broader concerns from stakeholders included:

1. Addressing a safeguard against policy changes;
2. Engaging the education minister and influential positions within Government;
3. As mentioned, state level changes are pointless – "we need to go national";

4. Coming from industry, they themselves understand the need to be involved at all levels and stages, but do not possess the know-how to access the leaders in charge; and lastly,
5. Addressing as a matter of national urgency the “weak passwords endemic” if there was not a national public awareness campaign.

SECTION SUMMARY

A double standard from a governance perspective exists with school-level control for both school cyber security and learning. Because responses are individualised across public, independent, Catholic, and other educational jurisdictions, an overarching coordinated response dictates that modification is the jurisdiction of state if not national government.

Equity of access is a barrier to state cyber security. Some schools gain little to no access to specialist staff in primary schools, and technicians for software and hardware issues are expensive. Ideally, all WA students should have equitable access to digital devices, because learning about and overcoming cyber threats protects students from cyber bullying and the implications of exposure to unregulated online company behaviour.

There is a need to maintain privacy online and this must be taught as part of the curriculum as well as within any public awareness campaign. Online safety is another key area to be addressed because negative psychological, neurological, and physical impacts are happening to us all individually from our online experiences. Anxiety and stress in our children is increasing at a cost to society and to government. Broader factors also require consideration toward curriculum inclusion and public awareness, such as safeguarding against policy changes; engaging the education minister and influential positions within Government; state level changes need to be addressed nationally; and lastly, to address as a matter of national urgency the “weak passwords endemic”, if there was not a national public awareness campaign.

Teachers’ experiences

Safeguarding teacher wellbeing

Protecting teacher wellbeing was an absolute priority for stakeholders, measured by each workshops’ group independently beginning conversations by acknowledging teachers and the important role they fulfil; despite conditions surrounding overloaded timetables, under-supported or stressed students, the crowded curriculum, and ongoing training requirements and standards. Workshop participants also commented on cyber security for teachers being an Occupational Health and Safety issue affecting psychosocial well-being.

Curriculum changes need to be timely to maintain a level of teacher care. Stakeholders are proposing an order of events whereby change does not start with teachers, or even with schools. The infrastructure for community awareness (such as a national health campaign) is ideally in place prior. This approach supports teachers and reduces the likelihood of teachers shouldering the burden, workshop stakeholders asserted.

Readily available professional learning

Educators want professional learning. There are many online resources. For instance, The Australian Cyber Security Centre (ACSC) and eSafety Commissioner offer courses on cyber security and safety online respectively, targeted for educators. A wide gap exists between that readily available cyber awareness knowledge or courses and that which reaches teachers. Furthermore, teachers do not need to be searching for courses. They do not have the time or inclination. Hence professional learning requires coordination and streamlining. Stakeholders acknowledged that schools and jurisdictions

already have key priorities, and match that with the professional learning they endorse and provide in their schools.

The Interim Report outlined (and was reinforced from workshop attendees) that there are a lot of resources available for educators and schools to access from both overseas and within Australia.

Teaching 'out of field'

Many secondary teachers are teaching 'out of field' and there are few digital technology specialist teachers. Other examples heard in the workshops include the earlier raised concern of how much is left up to individual schools, with the administration of one school informing a Humanities and Social Science teacher that she "ticked the box" for teaching students coding. But she herself didn't think that.

Teacher professional learning + culture building

Professional development can afford to be focused on practicing learning within collaborative environments, engaging with colleagues and understanding the value of networking. Teachers learning within collaborative environments gives rise to developing common vocabularies, as well as learning to manage collaboration. These processes can be emulated within the classroom with students, as well as successfully engaging external industry professionals within the classroom. This idea leans toward a 'co-design' approach to curriculum implementation, where environments are being supported to become increasingly collaborative, wellbeing and leadership capacities increase for teachers, because connecting with others shifts groups into a supportive team mentality, co-design, and the management of learning environments at the teacher level. Culture can be strengthened by activating cross-learning area conversations between teachers. This opportunity speaks to teacher professional learning extending to the soft skills of teachers themselves.

Summing up the pertinence of overcoming barriers by addressing school internal culture was represented in a workshop attendee's statement as follows:

> *Primary school teachers are generalist teachers working across eight learning areas within a crowded curriculum. This is tough. There are great resources out there. But unless we are building a culture within the school, staff will say great, tell me what to do – through a continuum of learning, and then they will have to dumb it down.*

These examples offer an insight into the depth of the issue of cyber security in schools, outlining why a resolution is required that emphasises a greater scale beyond teachers' professional learning or even purely a whole school approach.

Obstacles to teacher professional learning

The obstacles to teacher professional development are well understood in terms of monetary constraints and teachers' availability. But the more specific issue of generating the environment within which cyber security professional learning is a priority, is not understood. An example explained was a cyber security business training package rolled out by tertiary education provider TAFE, consisting of three units at fifteen hours per unit. "But the conversation with teachers around that remains about how the training can be reduced down to two hours," stated a workshop attendee. The statement reflects the need for societal change and broader understanding. Because, they deduced, "Changing culture is not possible in two hours".

In terms of professional learning for teachers within the more technical realm, it was raised in the workshop that the Computer Science Education Research Group (CSER) based at the University of Adelaide in the School of Computer Science provides a Digital Technologies MOOC program offered for Australian teachers. One of the MOOC offerings is Cyber Security and Awareness – Primary Years at a cost of $99 AUD. This is complemented by a similar offering bespoke for Secondary Years teachers. Such courses are already cheap and accessible.

The ongoing nature of cybercrime insists on ongoing professional development, implying a one-day workshop will not work for instance. However, targeted workshops supported by ongoing modules have potential.

Teacher professional learning – aligning with career stages

Continuing, one attendee suggested aligning technical knowledge-based professional development with the four career stages as found in the Australian Institute for Teaching and School Leadership teacher standards. Resources for graduate level teachers could be provided which would be different to the resources provided for a lead teacher. This would require nationwide coordination and consultation. Another suggestion was staged progress based on teachers own identified level of abilities. Approaches to professional learning mentioned include:

- Modular
- Train the trainer
- Three free TAFE units available for teachers
- Mandate of digital cyber security licence
- CSER MOOCs (University of Adelaide)

SECTION SUMMARY

Teachers are already overwhelmed. The curriculum is crowded. WA adopted and adapted the Australian Curriculum version 8.4 and identified core and additional curriculum content to reduce the amount of curriculum teachers were required to implement. Safeguarding teacher wellbeing is a priority for stakeholders. Curriculum changes need to be timely and contribute to maintaining a level of teacher care. The infrastructure for community awareness needs to be in place prior to curriculum level change. Professional learning is readily available but requires coordination and streamlining. Stakeholders acknowledge that schools and jurisdictions already have key priorities, and match that with the professional learning they endorse and provide in their schools.

Resources can be targeted to the level of teaching, from graduate to lead teacher, requiring nationwide coordination and consultation, bearing in mind the need for change at the societal level. The ongoing nature of cyber-crime insists on ongoing professional development, implying that one-day workshops will not suffice but regular, ongoing professional learning is required.

Vital change in the curriculum

In addition to the points below, researchers heard that educational staff need the resources to augment relevant learning areas with aspects of cyber security.

Techniques / strategies for curriculum implementation

A well-received idea from several attendees was the concept of a ‘digital cyber security licence’, in the same way as in the ‘olden days’ we had ‘pen licences’ at school. This idea was extended within another workshop as being whole school based, whereby schools and/or teachers might receive a digital cyber security licence confirming their capacity to be cyber aware, cyber hygenic, cyber safe and cyber secure. There may be scope here to relate school-level digital cyber security licence into a national identity of digital citizenship.

Shared language, standardised and inclusive of ethics, privacy, and behaviours

As established earlier in the report, industry is hoping for a stable lexicon from which to build a shared understanding across all facets of our society in using devices online. It might follow that understanding would deepen by society more widely, given time.

Workshop attendees were asked specifically to respond to Table 1 (see below) of the Interim Report outlining the current language used to reflect knowledge and skills which we would now recognise as cyber security inclusion in the national curriculum. The researchers asked workshop participants, with each cyber security threat, do we need to include learning about this in the Australian curriculum? Table 1 references common security threats that the revised national curriculum version 9.0 has identified for individuals and families.

Table 1*: Interim Report.*
Inclusion of relevant skills and knowledge to teach common cyber security threats in the Australian Curriculum 9.0: Curriculum Area, Strand & Band

Common Cyber Security Threats	Learning Area/ General Capability, Strand & sub-strand	Content Description	Band
Crypto (Currency) Mining	**Digital Technologies** *Processing and production skills: Privacy and data security*	Develop cyber security threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Data Spill/Data Breach	**Digital Literacy** *Practising Digital safety and wellbeing: 2. Manage digital privacy and identity*	Recognise that their digital footprint is valuable, used by online tools for targeting, and that data shared online is no longer under their control	Level 5 (Years 7 & 8)
Denial Of Service (Ddos Attack)	**Digital Technologies** *Processing and production skills: Privacy and data security*	Develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Hacking	**Digital Literacy** *Practising Digital safety and wellbeing: 2. Manage digital privacy and identity*	Protect content when sharing by selecting appropriate access controls for individuals and shared links for wider groups	Level 5 (Years 7 & 8)
Identity Theft	**Digital Technologies** *Processing and production skills: Privacy and data security*	Access multiple personal accounts using unique passphrases and explain the risks of password re-use	Band 5-6

Malicious Insiders	**Digital Technologies** *Processing and production skills: Privacy and data security*	Develop cyber security threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Malware	**Digital Technologies** *Processing and production skills: Privacy and data security*	Develop cybersecurity threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Phishing – Scam Emails	**Digital Technologies** *Processing and production skills: Privacy and data security*	Explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cyber security threats	Band 7-8
Ransomware	**Digital Technologies** *Processing and production skills: Privacy and data security*	Develop cyber security threat models, and explore a software, user or software supply chain vulnerability	Band 9-10
Scams	**Digital Technologies** *Processing and production skills: Privacy and data security*	Explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cyber security threats	Band 7-8
Web Shell Malware	**Digital Technologies** *Processing and production skills: Privacy and data security*	Develop cyber security threat models, and explore a software, user or software supply chain vulnerability	Band 9-10

Attendees offered specific feedback regarding the threats listed, mounting to the researchers' comprehension that there are other areas of threats not listed, and those listed are not necessary for families to comprehend, or at least not at the detailed level presented. For instance, crypto (currency) mining is "not general enough", one industry attendee mentioned, continuing by saying that it "may not be the thing in five years' time". And then, "this list is a combination of actors, mechanisms and affects", for which an educator replied, "this list will scare teachers."

More than one workshop received a very strong affirmative response upon hearing from individuals that an ethical understanding of acting within cyber space was important to be included in such a list, as well as the psychological behaviour of criminal activity.

Attendees approved of cyber security items being included much earlier than for years 11 and 12. There is evidence of aspects of cyber security currently embedded across the learning areas. But "we need the language around the tech as well as the behaviour to be (referred to in a) standardised (manner)", attendees concurred. Another workshop heard that a "basic baseline of the language beyond generic is required before students get issued a laptop".

At the outset, the new national curriculum 9.0 (released April 2022) aligns more closely with the needs of tertiary and industry with further clarity differentiating between key concepts such as cyber-safety, cyber awareness, and cyber security. For instance, Table 1 makes clear there are only two security threats identified in the Curriculum Version 9.0, whilst the other threats are not addressed until year 7.

Not learning anything about staying secure online until children are 11 or 12 years of age appears too late, before then moving abruptly in the following year to learn about scams, phishing, data breaches and hacking.

Ethical hacking is a widespread approach within the cyber security industry utilised to identify criminality through patterns of behaviour, as well as for office workers learning cyber security e.g., a cyber security company sending phishing emails to their client company's staff to expose to employees how they would have enabled a system breach.

Ethical hacking has been successfully applied as the key learning approach taken by organisations teaching high school students and beyond. For instance, by way of lesson plans, games and projects outlining what one can do within the law, one Australian organisation (who developed the internationally recognised OSSTMM framework outlining cyber security methodology) created the Hacker High School website presenting across multiple languages with millions of downloads annually. Consideration should be given to the possible implications of employing ethical hacking as students exposed to it sometimes engage in offensive hacking [19], although positive and ethical peer group culture is a key driver in student decision making, and the context or type of environment in which learning takes place is key [20].

Furthermore the vocabulary is broad rather than explicit around cyber security within the Management and Operations element itself, explaining the sub-element of Manage Online Safety including stating, "students develop the appropriate … skills to address online risks", implying that online safety and risks fall under the same bracket, whilst in Manage Digital Wellbeing there is no mention of cyber security, although the other areas mentioned are pertinent in relationship to what has been identified as important by stakeholders. In this way the curriculum will benefit from a standardised lexicon.

Overall, use of a systemic and progressive language is the way forward for students. For example, 'python façade' for cyber security moves into robotics. Students learn how to make robots and that may progress into a Cert IV Robotics, the researchers heard.

SECTION SUMMARY

Educational staff need the resources to integrate cyber security within the current learning areas. A helpful suggestion made was the concept of a 'digital licence'. Schools and/or teachers receive a digital cyber security licence confirming their capacity to teach cyber safety, cyber awareness, and cyber security on a progressive scale. A shared language is required to develop shared understanding and meaningful collaboration. Industry wants a stable lexicon, standardised and inclusive of ethics and behaviours.

Ethical hacking has been successfully applied as the key learning approach taken by organisations teaching high school students and beyond, for instance, by way of lesson plans, games and projects outlining what one can do within the law.

Insights into the WA Context

The text below provides insight into the WA context provided by the School Curriculum and Standard Authority (SCSA). Consultation with representatives from SCSA occurred in January 2023 (and is ongoing).

In September 2015, Australia's education ministers endorsed the Foundation (Pre-primary) to Year 10 (F–10) Australian Curriculum (version 8.4) developed by the Australian Curriculum, Assessment and Reporting Authority (ACARA). After consultation with teachers and other important stakeholders, Western Australia 'adapted and adopted' the F-10 Australian Curriculum:

- Adapting – changing parts of the Australian Curriculum i.e., re-writing or editing content descriptions and/or achievement standards, or retaining original content
- Adopting – copying a content description and/or an achievement standard.

Since 2015, the eight learning areas (listed in Table 2 below) from version 8.4 have been adapted and adopted to become the Western Australian Curriculum and Assessment Outline.

Western Australian Technologies curriculum

The Technologies curriculum is written on the basis that all students will study both Technologies subjects (Digital Technologies and Design & Technologies) from Pre-primary to the end of Year 8. Within Design and Technologies (Engineering principles and systems; Food and fibre production; Food specialisations; Materials and technologies specialisations), students have the opportunity to study at least one of the contexts. In Years 9 and 10 the study of Technologies is optional (referenced by the table's single asterisk).

	Hours per week over 40 weeks per year *(based on a 25 hour school week*)*			
	Pre-primary –Year 2	**Years 3–6**	**Years 7–8**	**Years 9–10**
English	6	6	3	3
Mathematics	5	5	3	3
Humanities and Social Sciences	2	2	3	3
Science	2	2	3	3
Health and Physical Education	2	2	2	2
Languages*	0–2	2	2	0–2*
Technologies*	2	2	2	0–2*
The Arts*	2	2	2	0–2*
Unallocated time**	2–4	2	5	5–11
Total Time	**25**	**25**	**25**	**25**

Table 2: *Notional teaching time allocated to each learning area (Pre-primary to Year 10).*

Senior Secondary Computer Science Syllabus

The Years 11 and 12 syllabus review process for the Computer Science ATAR course was completed in 2022. The Computer Science Curriculum Advisory Committee consisting of representatives from the school systems/sectors, university sector, practising teachers, industry, and professional associations reviewed and revised the syllabuses. Two public consultation opportunities occurred during the process. The first was to seek feedback on the existing Years 11 and 12 syllabuses and the second was to seek feedback on the proposed revisions to the syllabuses. Consultation drafts of the proposed Years 11 and 12 Computer Science ATAR syllabuses were directly sent to all WA universities to provide feedback. All schools currently implementing the Years 11 and 12 Computer Science course were asked to indicate their support for the revised syllabuses. This is a standard practice where a 75% acceptance rate is expected by the Authority Board before endorsement. 100% acceptance rate was received.

The new Year 11 Computer Science ATAR syllabus will be implemented in 2023 and Year 12 Computer Science ATAR syllabus in 2024. Cyber security concerns including identifying threats and mitigation are included within the Computer Science course. Western Australia is the only jurisdiction to have a Years 11 and 12 course that includes content related to cyber security.

SCSA has completed a detailed audit of the endorsed Australian Curriculum version 9.0 (endorsed by Education Ministers on 1 April 2022) against the current Western Australian curriculum.

SCSA has developed a Business Case for the WA state Government's consideration. As part of the State Government's 2023-24 Budget, $24.3 million has been committed to support the Authority to adopt and adapt the Australian Curriculum Version 9.0 within the Western Australian Curriculum and Assessment Outline. This will involve the following activities:

- reviewing and revising the current Western Australian curriculum (adopt and adapt)
- consulting with teachers and other stakeholders on the revised curriculum (consult)
- updating relevant teacher support resources for all learning areas, subjects and year-levels Pre-primary to Year 10 (curate existing resources)
- creating new teacher support materials to support teachers to implement the new content descriptions and to assess and report student achievement (develop assessment tasks)
- developing and delivering professional learning for all learning areas (develop professional learning/deliver professional learning)
- quality assuring all curriculum materials, support resources, and professional learning materials (web development)
- developing moderation processes and materials (moderation)
- validating grade descriptions (validate).

Consultation feedback from secondary teachers on the Australian Curriculum version 9.0 included concerns about the overlap of the extra sub-strand of 'Privacy and Security' and content currently being delivered, compounding time constraint problems, and indication that the content would be better suited to sit within the Digital Literacy general capability.

Future considerations and constraints in the WA context

Currently no Western Australian university offers a Major in Digital Technologies in their Bachelor of Education degrees.

Cyber security knowledge and skills are available for students beyond Year 8. If Years 9–12 were mandated for students how would this be staffed in all Western Australian schools?

Support for teachers and their professional learning

Teacher support related to the delivery of the Technologies curriculum is the responsibility of the educational systems' sectors (ASC, AISWA, DoE, CEWA). This is not the remit of SCSA. There is opportunity to enhance pre-service teacher education with cyber security knowledge, skills and understanding, however, initial teacher education programs are highly regulated with limited flexibility to incorporate additions.

It is proposed the researchers will investigate the professional development levels that teachers currently have in order to propose professional learning opportunities that will meet the needs for a) teachers' personal cyber awareness, cyber safety and cyber security, b) how to augment the curriculum to confidently include aspects of cyber security when teaching students, and c) increase self-efficacy to teach relevant cyber security content at appropriate developmental levels.

A top-down approach supported by bottom-up consultative process for systemic adaptations to augmented curriculum

Figure 5 outlines the big picture of actionable deliverables following along the processes of building, dialoguing, and finally production processes (refer to key), required to achieve curriculum augmentation and cyber security awareness. The figure represents a top-down approach supported by bottom-up consultation to meet the cyber security needs of the nation. Whilst this report considers the Western Australian position, the trajectory of deliverables addresses the national space for the optimal outcome. The strength of this approach is in arriving at the solution through both stakeholders and preliminary international findings whilst fundamentally supporting teachers and schools and the internal culture within educational settings and addressing the shortage of a skilled workforce.

LEXICON DEFINED – We elevate and streamline cyber industry knowledge by making known and valued the need for cyber awareness, cyber hygiene, cyber safety, and cyber security.

STREAMLINE ACCESS – Equity of access to digital devices and technical support across the state will remain a barrier until government generates a system whereby resources and technicians are accessible within an ongoing capacity throughout schools inclusive of regional/remote.

LEADERS TAKE RESPONSIBILITY - Computer science's know-how of the 'trickledown effect' deploys an approach through augmenting the curriculum to achieve national digital security through auditing school cyber practices (reducing the risk of being targeted) which trickles down through teachers, students, families then the public including individuals and companies whose leadership would then also be held responsible for their cyber security in a similar manner.

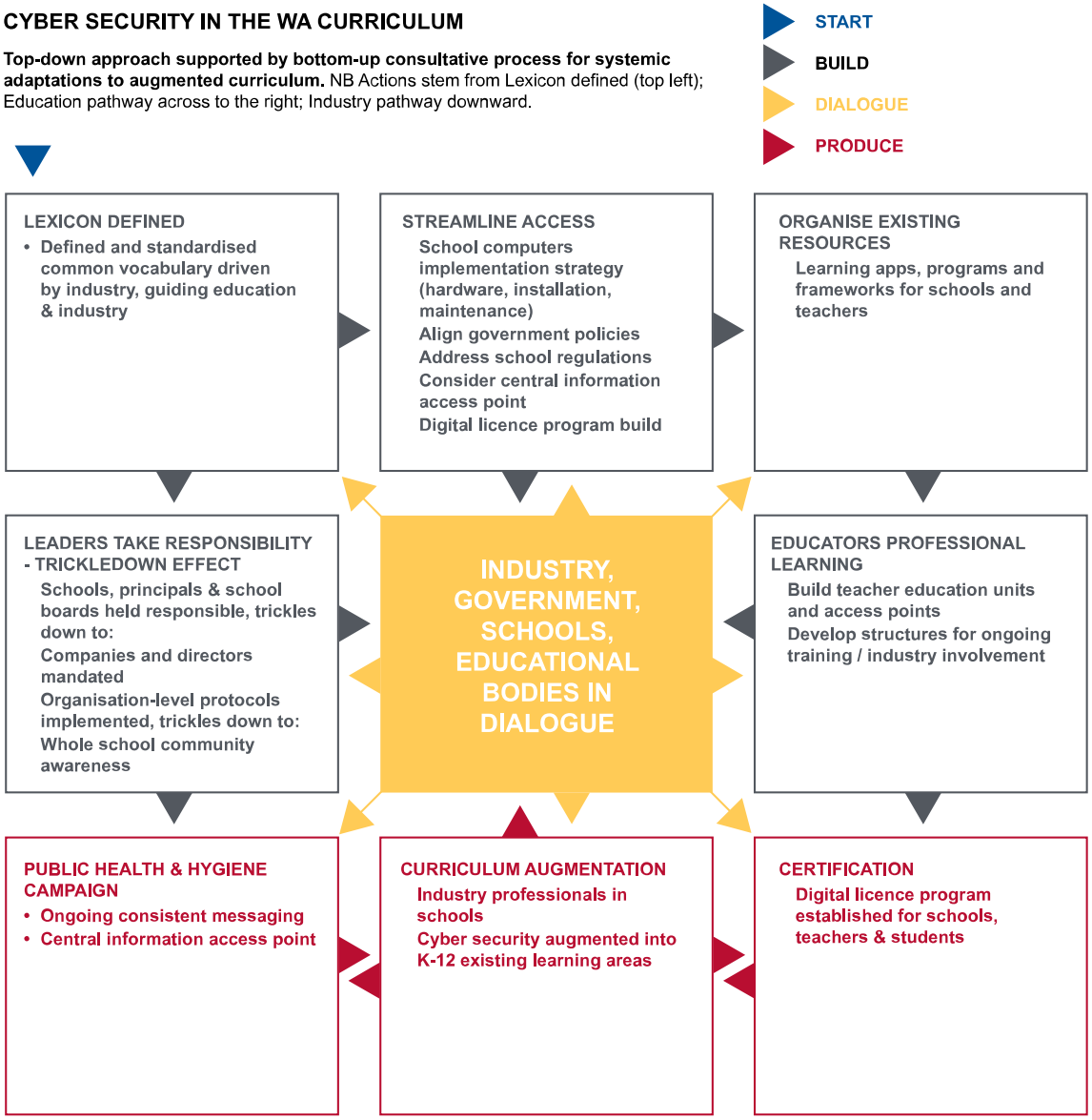

Figure 5: Big picture of actionable deliverables

EDUCATORS PROFESSIONAL LEARNING, RESOURCES and DIGITAL CYBER SECURITY LICENCE CERTIFICATION - Professional learning and learning resources are both readily available but necessitates nationwide coordination and streamlining (and in an ongoing capacity), also recommended to be addressed in the next phase of this project initially by way of consultation. Resources can be targeted to the level of teaching, from graduate to lead teacher. A digital cyber security licence purports to signify schools' teachers' and students' competencies in computing areas, supporting national identity around digital citizenship. The project extension proposes to identify how this licence could be implemented and what is required.

PUBLIC HEALTH AND HYGIENE CAMPAIGN – As leaders take responsibility and other structural changes occur, implementing a national campaign activates and reinforces the necessary behavioural changes and the importance of those shifts, engaging all levels of the education system's personnel towards safer and more secure online activity.

CURRICULUM AUGMENTATION - A collaborative approach with industry through an augmented curriculum ensures learning content remains relevant, because after curriculum changes *are* made, they remain open and adaptable. Stable educational structures are fundamentally incompatible with cyber. An augmented curriculum through cross-sector collaboration focuses on ongoing partnerships with industry professionals inside of schools, igniting student interest toward choosing technical elective units in middle upper school.

K-12 LEARNING AREAS - The report findings confirm that cyber security is best viewed not as its own subject because not only would another learning area be competing for time, but the nature of digital devices and their use is adaptable across many learning areas. Educational staff will require the resources to integrate cyber security where relevant across the learning areas.

Positive advances in Western Australia include cyber security learning added into the 2023 Computer Science ATAR syllabus and is the only Australian jurisdiction to have a Year 11 and 12 course that includes content related to cyber security. But we must start at as early as age 5 to embed desired behaviours, mitigate risk and build national digital citizenship. This research project's extension is proposed to include an outline identifying the best resources already available. Digital Technologies as an elective unit from year 9 onwards is proposed to be reconsidered with most students missing out on important content significant to safety and security.

Considerations and recommended actions

The report points out some considerations for immediate action:

- A national cyber security public health campaign targeting year 7 – 12 students. There are three key behaviours needing to be encouraged from the top down:
    1) using a password manager;
    2) multifactor authentication; and,
    3) updating devices.
- A national dynamic digital cyber security licence for students, teachers, and schools.
- Consultation with principals to identify professional learning needs of their staff.
- Teacher professional learning to develop knowledge of cyber awareness, hygiene, safety, and security.

Next steps

It is proposed that the ECU research team work on designing a 1-2-minute video and a poster to provide the first step for a proposed national cyber security public health campaign. It would be targeted to year 7 – 12 students and feature the three key behaviours as stated above, alongside reference to websites where additional help can be sourced. While the project would not be able to cover television advertising, it could be easily supported via a social media campaign. Furthermore, it is proposed the ECU research team design the dynamic digital cyber security licence for roll-out to WA students, teachers, and schools, followed by a national roll-out across Australia. This licence would be developmental and encompass basic levels of cyber hygiene and cyber awareness, moving towards higher and more sophisticated levels of cyber safety and cyber security. Both actions would be informed and shaped through consultation with key stakeholders including WA school principals. The consultation paper proposed to be delivered as part of the new project will moot these two actions and then seek insight from principals as to the professional learning needs of their staff surrounding cyber hygiene, cyber awareness, cyber safety, and cyber security. From there, as part of a top-down approach, principals can select the best professional learning options for their staff and incorporate this professional learning as part of their school-wide planning. It is proposed these deliverables will comprise the proposed one-year extension of scope to the current project.

Conclusion

Through the various research processes this project substantiates analogous findings across stakeholder consultation, initial literature reviews of cyber security initiatives within curriculum and schooling including international approaches, and the writing of this report. Alongside of identifying additional deliverables within the confirmed project extension, conclusions are outlined below.

International studies present that school curricula hardly pays attention to cyber security and computer science more broadly, and there is reinforcement from Western Australian stakeholders echoing the need for the new Australian curriculum to address the specifics required to achieve student digital citizenship.

Providing adequate cyber security skills and knowledge has been found to present nationwide and local challenges for all countries considered within the initial systematic literature review; those challenges often falling beyond the scope that K-12 schooling and curricula can be expected to attain. Because the nature of cyber security is ubiquitous, the absence of understanding about its importance impacts not only students but also every person online, highlighting the need to address the lack of awareness as the main challenge to overcome. Moreover, the immediacy of cyber threats exponentially grow due to a lack of a cyber workforce, relevant teacher education and professional learning, and the pace of technological shifts.

Initial findings of movements abroad and within Australia speak of countries' communities and cyber security industries being the primary instigators for cyber security in schools (and higher educational institutions) through initiatives spanning applied frameworks, courses, and training. Frameworks are designed to address either the severe shortage of a skilled cyber workforce through training programs for educators and/or students, or educational institutions' security weaknesses/protocols surrounding security, with educational institutions being specifically targeted by cyberattacks. This paper is among the first of its kind, offering a comprehensive overview of cyber security in school curricula, informed by international literature, and addressing a wide range of concerns.

Internationally and in Australia individual educators and some schools are taking on board the training being instigated by industry, success measured by students entering further education in cyber because of it. The training has shown to provide one effective approach but still relies on individual schools' or teachers' instigation and does not address teacher wellbeing and staff retention, nor a content-heavy curriculum. Locally teachers' incidental cyber knowledge sets are being 100% relied upon to fulfil their duties imparting cyber curriculum content. Hence it is suggested that a nationwide coordinated approach to streamline existing teacher professional learning resources occurs, in line with the other actions outlined here. Coupled with the creation of a developmental dynamic digital cyber security licence for students, teachers and schools, these strategies can increase awareness, knowledge and greatly mitigate against the many cyber risks society faces.

The changes required to build a workforce can be considered as inevitable because industry has already initiated it. Whether curricula and education systems accept industry's knowledge and assistance or not, the changes to education are already upon us. The question is more so whether (state and other) education is ready to regain relevance through an augmented approach akin to the rest of the evolving adaptive system, currently forming from the ground up.

The societal-wide lack of digital literacy coupled with low-level digital security has increased the risk individuals unknowingly endure when on devices within our workplaces, schools, and homes. It is a rife, worldwide societal endemic. A national awareness campaign like Slip Slop Slap is proposed, to reduce that risk of loss of identities, livelihoods, and lifestyles, with the risk extending to data and machinery hardware foundational to the economic and organisational structures supporting productivity. In staying attentive to the scope of this project, the intent in proposing investment in widespread behavioural

change via a national campaign aligns with the level of threat presented within stakeholders' adamance that this is a national public health crisis. The approach paves the way for widespread impact by rapidly resolving: the crises in the tech workforce and specialist teacher shortages; school and business' cyber security and responsibility; and student wellbeing online, because security would be valued and understood. Further momentum is required for which the project extension could support. Government agencies or departments are ideal at leading a collaborative effort required for a public awareness campaign across industry and education because of their authority, backed by state if not national budgets. We build a common vocabulary and kickstart the culture engaging people to shift their online behaviour by normalising it. Neither industry nor schools can implement curriculum change nor build a skilled cyber workforce fast enough to address the exponential growth of cyberattacks without a coordinated nationwide top-down approach, one attuned with bottom-up led processes, for instance in implementing the findings from this report.

Addressing cyber security in schools through augmentation of the curriculum enables schools to recoup relevance before being left further behind in losing students to community and industry-led cyber training attempting to fill the gap of a cyber skilled workforce. As we do want Australian citizens to develop a deeper level of skills and understanding of the ways in which threats to cyber security might specifically cause harm (in the ways that are outlined by ACSC). However, the task at hand is greater than simply incorporating more curriculum content, leaving teachers left to shoulder the burden of a national cyber security crisis.

References

[1] Witsenboer, J. W. A., Sijtsma, K., Scheele, F. (2022) Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186:104536. DOI: *10.1016/j.compedu.2022.104536*

[2] Hipsky, S., Younes, W. (2015) Beyond Concern: K-12 Faculty and Staff's Perspectives on Privacy Topics and Cybersafety. International Journal of Information and Communication Technology Education, 11(4). DOI: https://doi.org/10.4018/IJICTE.2015100104

[3] Venter I.M., Blignaut R.J., Renaud K., Venter M.A. (2019) Cyber security education is as essential as "the three R's". 5(12)

[4] Pike, R. E., Curl, S. S. (2013) The "Ethics" of Teaching Ethical Hacking. Conference on Information Systems Applied Research, San Antonio.

[5] Nix, C. A., Ward, J., Fontecchio, A., Ruddick, J. (2014) Using the Similarities Between Biological and Computer Virus Behavior to Connect and Teach Introductory Concepts in Cyber security in a Biology Classroom. IEEE Frontiers in Education Conference. DOI: *10.1109/FIE.2014.7044028*

[6] Education News Canada (2021) Canada's largest cybersecurity education program for high schools launches in partnership between Cisco and STEM Fellowship. *https://educationnewscanada.com/article/education/level/k12/3/932072/canada-s-largest-cybersecurity-education-program-for-high-schools-launches-in-partnership-between-cisco-and-stem-fellowship.html*

[7] Kamaludeen, M., Ismaeel, S., Asiri, S., Allen, T., Scarfo, C. (2020) A Framework for Cyber Protection (FCP) in K-12 Education Sector. *https://doi.org/10.1049/icp.2021.0865*

[8] Moore E., Likarish D., Bastian B., Brooks M. (2021) An Institutional Risk Reduction Model for Teaching Cybersecurity. IFIP Advances in Information and Communication Technology, 615. DOI: 10.1007/978-3-030-80865-5_5 *https://link.springer.com/chapter/10.1007/978-3-030-59291-2_2*

[9] Pusieski, M. (2017) Cyber Security in Canada's Schools: An Interview with Benjamin Kelly. *https://www.tripwire.com/state-of-security/cyber-security-canadas-schools-interview-benjamin-kelly*

[10] Department of Education and Early Childhood Development, New Brunswick (2019) Cybersecurity 120. *https://www2.gnb.ca/content/dam/gnb/Departments/ed/pdf/K12/curric/TechnologyVocational/Cybersecurity120.pdf*

[11] Kohgo, A. (2014) Information security education for students in Japan. National Institute for Educational Policy Research Japan. *https://www.nier.go.jp/English/educationjapan/pdf/201403ISE.pdf*

[12] Alderman, T., Ariel, B., Harinam, V. (2023) Can a Police-Delivered Intervention Improve Children' Online Safety? A Cluster Randomised Controlled Trial on the Effect of the "ThinkUKnow" Programme in Primary and Secondary Australian Schools. Journal of Experimental Criminology. DOI: *10.1007/s11292-023-09551-3*

[13] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ (Clinical research ed.), 372, n71. *https://doi.org/10.1136/bmj.n71*

[14] Cyber.org (2021) CYBER.ORG Releases First National K-12 Cybersecurity Learning Standards. *https://cyber.org/news/cyberorg-releases-first-national-k-12-cybersecurity-learning-standards*

[15] Lucariello, K. (2022) Virtual Lab Environment Cyber.org Range Launched to Make K–12 Cybersecurity Skills Training Available Nationally. *https://thejournal.com/articles/2022/11/30/virtual-lab-environment-cyber.org-range-launched.aspx*

[16] Kritzinger, E., Bada, M., Nurse, J. R. C. (2017) A Study Into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK. Information Security Education for a Global Digital Society, pp. 110–120. Springer, Cham. DOI: *10.1007/978-3-319-58553-6_10*

[17] Yılmaz, R., Yılmaz, F. G. K., Öztürk, H. T., Karademir, T. (2017) Examining Secondary School students' Safe Computer and Internet Usage Awareness: An Example from Bartın Province. Pegem Journal of Education and Instruction, 7(1):83–114. DOI: *10.14527/pegegog.2017.004*

[18] O'Neil, C., Penn, A., Hupfeld, M,. & Falk, R. (2023) 2023 – 2030 Australian Cyber Security Strategy Discussion Paper. *https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/2023-2030-australian-cyber-security-strategy-discussion-paper*

[19] Trabelsi, Z. and H. Saleous, H. (2018) "Teaching keylogging and network eavesdropping attacks: Student threat and school liability concerns," 2018 IEEE Global Engineering Education Conference (EDUCON), Santa Cruz de Tenerife, Spain (437-444). DOI: 10.1109/EDUCON.2018.8363263.

[20] Pike, R. E. (2013) "The "Ethics" of Teaching Ethical Hacking," Journal of International Technology and Information Management: Vol. 22: Iss. 4, Article 4. DOI: https://doi.org/10.58729/1941-6679.1021 Available at: *https://scholarworks.lib.csusb.edu/jitim/vol22/iss4/4*