EAI Endorsed Transactions
on e-Learning

Research Article EAI.EU

Infusing Aboriginal Perspectives in Cyber Education

John Shannahan[1], Mohiuddin Ahmed[2]

[1]Centre for Learning and Teaching, Edith Cowan University, Australia
[2]School of Science, Edith Cowan University, Australia

Abstract

While human factors are important in cyber security, the discipline has largely not explored incorporating Indigenous perspectives—or, more specifically, in an Australian context, Aboriginal perspectives—in its curricula. In this paper, we introduce a promising approach for aligning Aboriginal perspectives with the needs of cyber security graduates and incorporating diverse perspectives into cyber degrees. The approach advocates for the centrality of good curriculum design fundamentals: backward design, constructive alignment, and student outcomes. The paper ends by reflecting on challenges and lessons from the first implementation and review of the material. It provides recommendations for other cyber practitioners exploring ways of incorporating Indigenous perspectives in their teaching.

Received on 15 March 2024; accepted on 20 February 2025; published on 30 April 2025

Keywords: First Nations' Perspectives, Indigenous Perspectives, Cyber Security, Cyber Education, Computer Science Education, Strength- and Deficit-based Discourse

doi:10.4108/eetel.5779

1. Aboriginal Knowledges and Perspectives in Australian Higher Education Curricula

For many years, Australia has pursued greater incorporation of Aboriginal knowledges and perspectives in its higher education curricula [1]. As a sector, we have come far enough that all our students should now expect to engage with Aboriginal content [1]. Nor are the drivers for increasing engagement limited to higher education bodies: the sector's position aligns closely with the efforts of Reconciliation organisations. Reconciliation Australia, for example, outlines five dimensions of reconciliation [2]. Three are especially relevant for higher education: equality and equity (that Aboriginal and Torres Strait Islander peoples "participate equally and equitably in all areas of life"), institutional integrity (that universities take concrete actions—within their sphere of influence—to support all dimensions of reconciliation), and historical acceptance (that institutions and individuals "understand and accept the wrongs of the past" and make "amends for past policies and practices" to ensure they are never repeated). These high-level principles manifest at universities in Aboriginal and Torres Strait Islander Strategies and Reconciliation Action Plans. In the institution discussed by this paper, for example, the first objective of the current strategic plan specifies that all students who graduate will "engage with Aboriginal and Torres Strait Islander content, perspectives, and histories" [3, 4].

Thus, in Australian higher education, we all have good reason to consider how we might incorporate Aboriginal knowledges and perspectives in our practice. Two key principles guide the design process: (i) new material should follow strengths-based discourse principles to avoid perpetuating stereotypes and negative impressions that have dominated discussion since colonisation [5, 6]; (ii) new material must align with the unit's learning outcomes and role within the course to ensure meaningful and relevant activities. Not all disciplines, however, appear to lend themselves to the incorporation of Aboriginal perspectives. For example, an academic in health sciences might discuss cultural determinants of health in a manner that closely relates to students' career destinations. By contrast, an academic teaching foundational programming languages may not see an immediate connection between Python and Aboriginal knowledge.

*Corresponding author. Email: j.shannahan@ecu.edu.au

While some STEM disciplines without an obvious connection to Aboriginal knowledges and perspectives have begun discussing options (e.g. Engineering [7]), cyber security educators have largely not explored how to improve in this space. We believe that this is a gap in our practice. Cyber security is now a national security priority for Australia [8]. Furthermore, at the time of writing, thirty-six of the forty-three universities in Australia offer cyber education programs. With the growing importance of our discipline, it is worth beginning the conversation about how we might incorporate Aboriginal knowledges and perspectives. It is a worthwhile conversation in itself, but broadening our discussions of non-technical skills will also significantly benefit our graduates. The importance of soft skills is not a radical idea or one restricted to Australian cyber education. The 2022 Employer Satisfaction Survey—collating responses from 3,452 graduate employers across Australia—rated "employability and enterprise skills" as the second most important way that qualifications could have better prepared graduates: above "technical and professional skills" [9]. Ultimately, students must learn the soft skills required to succeed in complex organisations.

Furthermore, contrary to some students' expectations [10], cyber security experts do not spend their professional lives sequestered away from others, working alone and exclusively focusing on technical issues. Part of our role as cyber academics is to dispel misconceptions about the profession and emphasise that a "well-rounded awareness of organisational culture and context are just as much, if not more important" than penetration testing and ethical hacking [11–13]. In this regard, as industry moves to combat stereotypes, improve gender diversity, and create more supportive work environments [14], so too must we as educators equip our graduates with the skills to collaborate with diverse stakeholders and understand organisational context.

The following, therefore, proposes an approach for introducing Aboriginal perspectives in cyber education. The approach significantly overlaps with non-Australian contexts where educators are working to decolonise curricula and incorporate First Nations' perspectives. Taking inspiration from calls for non-Indigenous people to take steps towards reconciliation by challenging themselves to learn and improve [15], our discussion reflects on the design process for a unit that trialed the incorporation of Aboriginal perspectives and identified lessons for others. Transcriptions of meeting brainstorms and minutes, interviews, personal reflections, and colleague feedback underpin these preliminary reflections.

2. Unit and Project Context

The work took place as part of a broader action-research project within a School of Science to (i) develop a process for supporting academics who would like to incorporate Aboriginal knowledges and perspectives in their units and (ii) increase student engagement with Aboriginal and Torres Strait Islander knowledges and perspectives.

The unit through which we infused Aboriginal perspectives focuses on enterprise security and governance. It is a third-year unit with enrolments in the Bachelor of Science (Cyber Security) and Bachelor of Information Technology programs. The unit enrolled more than 100 students per semester in the last three offerings. The unit focuses on enabling students to relate security frameworks to an enterprise context with a focus on governance. It also surveys approaches to contemporary cyber security issues within an enterprise environment.

3. Pedagogical Principles and Method

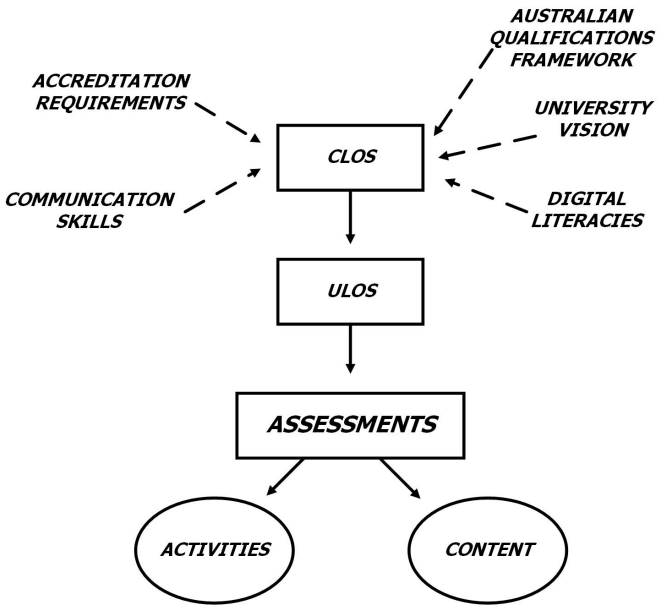

Figure 1. A simplified illustration of the components of backwards design

We predicated our approach on the roots of good unit design: constructive alignment [16] and backwards design [17] (Figure 1). The first step, before developing any new content, was to reflect on the course learning outcomes (CLOs) and unit learning outcomes (ULOs). We needed to ensure that they were meaningful, measurable, and achievable. In our case, the unit assured student attainment of two CLOs. The first, for the Bachelor of Science (Cyber Security), was "incorporate an awareness of cross-cultural issues

and demonstrate cultural and Indigenous competence in professional practice in the cyber security area." The second CLO, for the Bachelor of Information Technology, was "apply an understanding of diversity and a global outlook, including Aboriginal and/or Torres Strait Islanders' perspectives, when designing information systems." The unit learning outcomes aligned with these CLOs were "propose approaches for enterprise security governance and implementation of security standards, policies and procedures" and "appraise contemporary approaches to enterprise security." The important second step was to brainstorm (i) what behaviours and (ii) what thought processes we would to like to see in graduates. Brainstorming narrowed our focus and provided a reference point to which we could align all later activity. The process also helped us avoid two pitfalls the project team had encountered in conversation with staff. The first pitfall was to limit one's scope to finding Aboriginal knowledge of a particular subject to repeat in class. The second was to focus on finding an Aboriginal person to deliver content in class. In disciplines where Aboriginal knowledge of a subject-area is not obviously relevant (e.g. database design), forgetting to have a precise purpose for diverse perspectives can result in tokenistic and bolt-on material. Similarly, relying on an Aboriginal person to do the hard work (learning, refining, and teaching material) contradicts calls for faculty-based staff to take greater responsibility in Aboriginal matters and exacerbates the burden already placed on staff in central Indigenous units [18, 19]. Ultimately, critical reflection on learning outcomes kept us focused on what graduates needed from their experience.

The next step was to reflect on assessments and whether they provided opportunity to assess or provide feedback on attainment of the CLO and ULOs. Only after that point did we begin considering specific content or activities which would scaffold students to attain their outcomes.

4. Assessments and Content

While brainstorming, we quickly identified that although cultural responsiveness was a necessary facet of the successful attainment of the CLO, it could not be the sole focus of the work in the unit—neither the ULOs nor CLOs for students' degrees supported extensive training in that space. Instead, the process renewed our focus on practical skills students need to function in the workplace.

Figure 2 represents how the unit's components complemented one another. In our unit, we saw that we could adapt the final assessment to encourage students to reflect on diverse perspectives and specifically Aboriginal peoples in Western Australia. The task

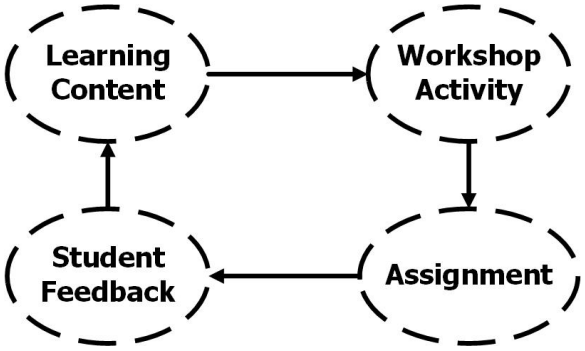

Figure 2. The unit components

requires students to respond to a case study. Students must first review a case study which outlines a business's function, size, and a recent cyber security incident. Students then role play as a cyber security consultant and produce a report for the business's executives which identifies key cyber loopholes, analyses root causes of incidents, and recommends appropriate solutions. We began drafting ideas for case studies which would allow students to reflect on business needs specific to a Western Australian context. The goal was to create several case studies for the the unit coordinator to rotate, with a view to front loading the workload: we wanted to avoid an unsustainable situation where the coordinator needed to develop new case studies for every teaching period in order to provide variety and reduce the likelihood that students would collude by working with previous submissions. Our first effort reflected on a mining company. This had the benefit of being an example (i) authentic to workplace destinations of our students, (ii) with complex organisational needs, (iii) reflecting an employer hiring individuals from a range of backgrounds, including Aboriginal and Torres Strait Islander peoples, and (iv) with business interests and locations in remote parts of the state.

The first case study, for example, included the following high-level details:

- The business's head office is in Perth, with mining sites dispersed across a region 1,000km distant.
- There are 1,000+ employees.
- Each employee has a unique ID card with RFID tags which also serves as an access card.
- There are only a handful of computers at mining sites. They do not have passwords.
- There is no IT or cyber awareness training culture.
- There is no multi-factor authentication.

- An employee used worksite computers to access his private email and saved a password in a notepad file. Recently, from this email address, company executives received enquiries from community Aboriginal organisations regarding donations and sponsorship. The business has worked with Aboriginal community groups in the past. The employee denied sending these emails.

- An employee working remotely asked for training with a .pdf letter. When opened by an employee in the head office, a ransomware notice appeared on screen and the computer was locked.

The case study provided several useful avenues for students to explore. For example, it is specific to an Australian cultural context where certain norms are essential; the employee numbers mean that students must consider users from a diverse range of cultural backgrounds and practices; employees are physically located in remote and in metropolitan areas; cyber security differs in remote and metropolitan locations for practical reasons.

The next task was infusing this thinking and material specific to Aboriginal peoples throughout the unit. In our planning stages, it was the act of dispersing these ideas which would (ideally) take our efforts from a bolt-on task at the end of semester to a well-aligned and useful experience. Figure 3 is our brainstorm illustrating how we moved from the assessment stage of backwards design to creating complementary content and activities.

Development proceeded from brainstorming along the following lines:

- Learning Content: It was important to retain focus on alignment of content with ULOs. We began by deciding which topics would be appropriate for Aboriginal perspectives. The unit's module on human factors was a natural fit. In this module, the unit coordinator designed short video lectures focusing on the need for understanding Aboriginal perspectives. We began breaking down student assumptions that human factors are irrelevant to working in cyber security. We used United Nations statements [20], CEO speeches [21], and higher education sector positions [1] to illustrate why understanding Reconciliation and diverse perspectives is essential for understanding complex organisations. A handout accompanied the videos, providing further references to the above, Reconciliation Australia resources, and other industry positions (including the mining sector's destruction of 46,000 year old cultural heritage sites [22, 23]. On the one hand, we were mindful of an instrumentalist approach wherein the value of engaging in Aboriginal and Torres Strait Islander knowledges and perspectives was couched solely in terms of student employment and personal success (as opposed to an altruistic good). On the other hand, from discussions with students, we were aware that some students—especially those from overseas—did not understand the connection between cyber security and Aboriginal perspectives and history. We continue to tread cautiously through this space and means of justifying these ideas to students. Overall, we follow Martin's note [24] that not all initiatives can be transformative in their first iterations. The important point, in this context, was beginning the discussion and challenging our students.

- Workshop Activity: Once the learning materials were finalised, we designed workshop activities to guide the students. In the case of the "human factors" module, we presented a case study with an Aboriginal business owner. Similar to the final case study, in this hypothetical business the owner didn't use passwords. In the context of different perspectives and training students to tailor solutions to specific business needs, the case study facilitated general discussion of cyber assumptions. It built on the research of Singh et al.[25, 26] into password sharing practices among different groups: people with disabilities, married couples, and Aboriginal peoples in remote locations [27]. The idea was to underscore a fundamental aspect of becoming a good cyber security expert: catering recommendations and explanations to each specific client. Not every client will have the same level of cyber security knowledge as an expert. In the simple case study above, for example, students should not assume that their clients automatically agree that the benefits outweigh the perceived costs involved in applying multi-factor authentication, character limits, and expiry rules. Good cyber security experts must be adept at creating compelling business cases for investing in their recommendations.

- Assignment: The students demonstrated their knowledge in the final task. In addition to a case study that provided avenues to explore Aboriginal perspectives, we also updated the marking rubric to allow markers to offer specific feedback on whether students dealt appropriately with the different needs and possibly practices of employees in a remote area.

- Student Feedback: During the teaching period and at the end of the teaching period, the

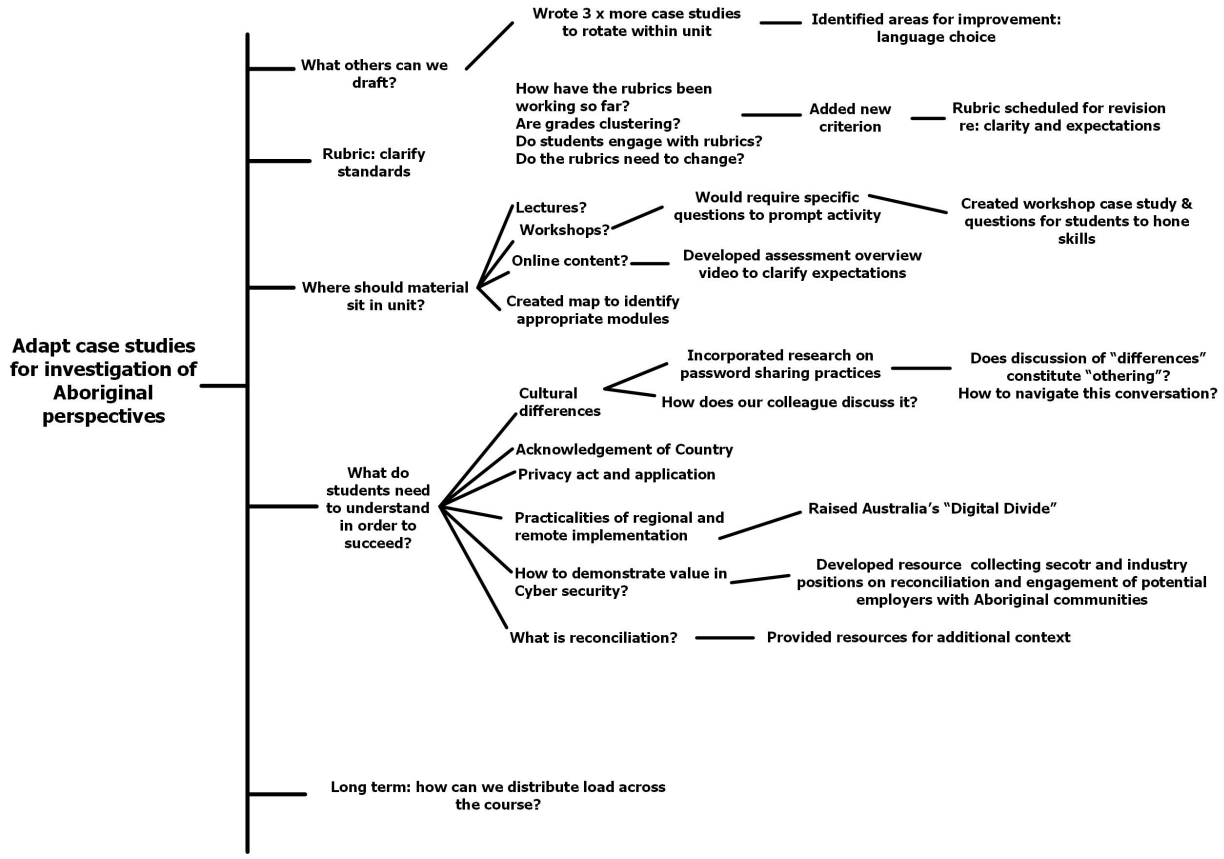

Figure 3. Copy of brainstorm to decide next steps.

unit coordinator informally asked students about the introduction of the Aboriginal perspectives. Anecdotally, most students accepted the need to know about these matters in the context of human factors in cyber security. Student feedback and our own reflections are now resulting in further refinement of the material and better alignment of content.

Overall, a broader aim was to introduce students to the complexities of working with different stakeholders and groups. Our efforts took place in the context of emphasising the importance of analysing and addressing business needs methodically. Discussing Aboriginal perspectives provided useful options to engage students in the thought processes they will need to employ in order to succeed when they enter the workforce.

5. Lessons for a Cyber Education Context

5.1. Avoiding Deficit-Based Discourse in a Deficit-Based Discipline

One of the first hurdles to overcome was that cyber security, in general, does not focus on positive traits. Cyber security experts naturally gravitate towards business and user deficiencies in confidentiality, integrity, and availability [28]. Discussing defence against cybercriminals and improving practice usually has no bearing on curriculum design. It does, however, create tension when discussing Aboriginal matters. Settlers have historically stereotyped Aboriginal people negatively and framed conversations in terms of disadvantage when compared to the rest of the Australian population [5, 6]. Deficit-based discourse—dialogue which emphasises or is framed around disparity, deprivation, disadvantage, dysfunction, and difference [29]—has impacted the writing of policy, legislation, and research in Australia and abroad [30, 31]. It is critical that we avoid it. The tendency to focus on difference perpetuates negative stereotypes and impressions of Aboriginal people; an audience with limited exposure to Aboriginal peoples or ideas would only have negative impressions on which to base their thinking. The ideal is to engage in the inverse: strengths-based discourse. The importance of avoiding deficit-based discourse created a delicate balancing act for unit development when this unit would typically require students to point out failures in business practices (e.g., open networks; poor

cyber hygiene) and employees (e.g., poor cyber awareness). Naturally, it is out of the question to frame any case studies or discussions in how a particular group is different to the rest of the country or dysfunctional in some way.

As an example of the challenge, we can reflect on a draft case study for the final assessment. It discussed a clinic with open WiFi networks that fell victim to a ransomware attack. One of the precipitants of the attack was a user clicking a lottery ticket scam while on the open network. A draft of the case study noted that the clinic employed Aboriginal staff members. However, two points quickly became apparent when discussing options with a colleague. First, specifying the ethnicity of staff members could be seen to be tokenistic and strange: when else would the ethnicity of a user-base be relevant or appropriate? Secondly, did the image of an Aboriginal individual tricked by a lottery scam imply that a particular group would be more likely to fall for a scam of that nature? It was an illustrative lesson in the importance of frank discussions with critical friends across the university. While it may have been perfectly unremarkable in another cyber context to comment on a user following a scam link, shoehorning an ethnic group into the discussion immediately caused concern. We scrapped the case study to focus on others with stronger foundations. The experience was a timely reminder that strengths-based discourse involves more than focusing on positive attributes; it emphasises sensitivity and reflection on perceptions, how we can improve, and maintaining a strict focus on only including material that serves a purpose for student learning.

5.2. Avoiding Stereotyping

The challenge of stereotyping manifested in the early stages of unit development. As we drafted new case studies of hypothetical businesses suffering from a cyber attack, we discussed the ideas with colleagues. One particular draft sparked a long discussion. The draft outlined a community-orientated business from a regional area. The business catered to the local Aboriginal community, providing legal advice as a registered centre, operating a domestic violence awareness program, managing a portfolio of properties, and serving as an employment recruitment centre. The business was a victim of a ransomware attack. One of the first reactions from colleagues was to ponder whether the draft used a stereotype of an Aboriginal business. Although the feedback seemed reasonable, it opened a new path for discussion because this case study was based on a real business operating in Western Australia and a genuine ransomware attack.

The conversation soon evolved into discussion about authentic scenarios and assessment, strengths-based discourse, and appropriate material. On the one hand, it was clear that the case study seemed to create a stereotypical "Aboriginal business." On the other hand, the business in question was real victim of a cyber attack which perfectly aligned with the unit's content and the roles students would need to take once they left university. Our discussions and reflections offered some excellent strategies for others writing new material. It is well known that authenticity is important and beneficial for student learning [32, 33]; it is therefore reasonable to use authentic examples. The excellent alignment of the draft to the unit's content meant that discarding the draft was unnecessary. It is, however, equally important to be mindful of stereotyping. In our case, the key to identifying where we had room to improve was focusing on what was crucial for student success in the task. While operating as a registered community legal advice centre provided an interesting avenue for students to explore in their assignment (it denoted that the information held at ransom was not only critically important to business operations and for privacy reasons, but retrieving and securing that data would have critical implications for the business's ongoing accreditation as a legal centre), the business's family-violence department served no purpose in the assignment or for student learning—it only furthered a stereotype that a "normal" Aboriginal business would operate in this space. The key lesson was always to be mindful of cultural issues and discuss ideas with as many colleagues as possible. Just as above, where the lesson was about the importance of including only material with purpose, in this case, we needed to remain conscious of the relevance of our material.

Another valuable idea from a colleague in Kurongkurl Katitjin, the university's Centre for Indigenous Australian Education and Research, was to explore business directories listing businesses owned and operated by Aboriginal men and women. After appropriate scaffolding, designing, and critically reflecting on Aboriginal material in a unit, if necessary and valuable to the base discussion around an Aboriginal business, these repositories may provide inspiration that will mitigate the likelihood that one will unintentionally fall into a description of a stereotypical business. We encourage readers not to use real business names or websites without permission.

6. Conclusions and Future Works

Despite initial doubt regarding how Aboriginal knowledges and perspectives could align with cyber security topics, the above approach offers a promising way to overcome obstacles. By focusing on the ultimate goal

of advancing cultural responsiveness and reconciliation, we increase the likelihood of uncovering valuable opportunities. Continual self-reflection and input from trusted peers were crucial in addressing faults in our early thinking. By openly acknowledging our shortcomings and embracing a journey toward cultural responsiveness, we now feel confident in sharing a candid summary of our unit development process. We aim to offer our experiences, including reflections, setbacks, and lessons learned, to assist individuals in Australia and beyond who are striving to incorporate diverse perspectives in technical disciplines and require guidance. A crucial next step in our institution will be further infusion of Aboriginal and Torres Strait Islander perspectives in other units: the risk at this stage is that the information is isolated to the case study outlined here. For effective assurance of learning, we aim to have material dispersed across the curriculum which introduces, consolidates, and asks students to demonstrate knowledge. To this end we have begun work with other unit coordinators following the same process described above. The goal is to avoid the perception that the material is a "bolt on" to the course, to provide a variety of ways to engage with Aboriginal and Torres Strait Islander material, and avoid a situation where one academic is responsible for the majority of the work in this space. Future research can then focus on evaluation of student knowledge after multiple opportunities to engage and alignment of our process with those being explored elsewhere in Australia (for Aboriginal and Torres Strait Islander contexts) and overseas (in First Nations contexts).

References

[1] "Indigenous strategy 2022–25," *Universities Australia*, 2022. [Online]. Available: https://rb.gy/4yxo5p

[2] "What is reconciliation?" *Reconciliation Australia.*, 2023. [Online]. Available: https://tinyurl.com/3jf23yak

[3] "Aboriginal and torres strait islander plan 2022–2026," *Edith Cowan University*, 2022. [Online]. Available: https://tinyurl.com/ye94ddhp

[4] "Curriculum design." *Edith Cowan University*, 2023. [Online]. Available: https://tinyurl.com/3yht5974

[5] C. Fforde, L. Bamblett, R. Lovett, S. Gorringe, and W. Fogarty, "Discourse, deficit and identity: Aboriginality, the race paradigm and the language of representation in contemporary australia," *Media International Australia incorporating Culture and Policy*, vol. 149, pp. 162–173, 2013.

[6] M. L. J. H. M.-J. Fogarty, William; Lovell, "Deficit discourse and strengths-based approaches: changing the narrative of aboriginal and torres strait islander health and wellbeings," *Lowitja Institute*, pp. 1–48, 2018.

[7] G. T. L. E. M. T.-K. P. J. . D. L. Kennedy, J., "A beginners guide to incorporating aboriginal perspectives into engineering curricula." 2016. [Online]. Available: https://tinyurl.com/at9dh7rc

[8] "Expert advisory board appointed as development of new cyber security strategy begins." *Department of Home Affairs.*, 2022. [Online]. Available: https://tinyurl.com/29jbecbr

[9] "2022 employer satisfaction survey." *QILT*, 2023. [Online]. Available: https://tinyurl.com/2hduke5n

[10] J. Wray, "The stereotype of cyber security." 2022. [Online]. Available: https://tinyurl.com/3ydnnp3d

[11] L. Harjinder, S. Jane, J. Mike, J. Helge, P. Blaine, and H. Richard, "Pedagogic challenges in teaching cyber security – a uk perspective," 2022.

[12] J. Allison, "Devising a cyber security management module through integrated course design," *Journal of Further and Higher Education*, vol. 47, no. 10, pp. 1389–1403, 2023.

[13] J. T. F. on Cybersecurity Education, *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY, USA: Association for Computing Machinery, 2018.

[14] L. Risse, M. Beamond, J. Hall, Y. Wang, M. Warren, B. Barua, and V. Kondylas, "Gender dimensions of the australian cyber security sector - report," Melbourne, Australia.

[15] B. Bennett, "The courage to feel uncomfortable: what australians need to learn to achieve real reconciliation," *The Conversation*, 2022. [Online]. Available: https://shorturl.at/jFGNX

[16] J. Biggs, "What the student does: teaching for enhanced learning," *Higher Education Research & Development*, vol. 18, no. 1, pp. 57–75, 1999.

[17] T. Angelo, *Designing subjects for learning: practical research-based principles and guidelines*, 2012, pp. 93–111.

[18] L.-I. Rigney, *A Design and Evaluation Framework for Indigenisation of Australian Universities*. Singapore: Springer Singapore, 2017, pp. 45–63.

[19] "Embedding aboriginal and torres strait islander presence: Opening knowledge pathways," *Australian Department of Education.*, 2011. [Online]. Available: https://shorturl.at/yzCR3

[20] "United nations declaration on the rights of indigenous peoples," *United Nations*, 2007. [Online]. Available: https://rb.gy/1mllum

[21] "Unfinished business - andrew mackenzie chief executive officer bhp." *BHP*, 2019. [Online]. Available: https://cutt.ly/Ww7cT4jB

[22] C. Wahlquist, "Rio tinto blasts 46,000-year-old aboriginal site to expand iron ore mine," *Sydney Morning Herald*, 2020. [Online]. Available: https://rb.gy/zs3hth

[23] N. Toscano and H. Hastie, "Rio tinto ceo, top executives resign amid cave blast crisis," *The Guardian*, 2020. [Online]. Available: https://shorturl.at/xE248

[24] M. K. L., "The role of aboriginal knowledges in higher education in the 21st century," *Department of Education, Skills and Employment.*, 2020. [Online]. Available: https://shorturl.at/cgX19

[25] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong, "Security design based on social and cultural practice: Sharing of passwords usability and internationalization." Australia: Springer, 2007, p. 10.

[26] ——, "Password sharing: implications for security design based on social practice," in *Proceedings of the SIGCHI*

Conference on Human Factors in Computing Systems, ser. CHI '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 895–904.

[27] E. Rennie and T. Yunkaporta, "Aboriginal communities embrace technology, but they have unique cyber safety challenges," *The Conversation*, 2016. [Online]. Available: https://shorturl.at/qPQV6

[28] M. E. Whitman and H. J. Mattord, *Principles of information security*, sixth edition. ed. Boston, MA: Cengage Learning, 2018.

[29] M. Walter, R. Lovett, B. Maher, B. Williamson, J. Prehn, G. Bodkin-Andrews, and V. Lee, "Indigenous data sovereignty in the era of big data and open data," *Australian Journal of Social Issues*, vol. 56, no. 2, pp. 143–156, 2021.

[30] C. . M.-S. . S. L. Hyett, Sarah Louise ; Gabel, "Deficit-based indigenous health research and the stereotyping of indigenous peoples," *Canadian Journal of Bioethics / Revue canadienne de bioéthique*, vol. 2, no. 2, pp. 102–109, 2019.

[31] J. Bryant, R. Bolt, J. R. Botfield, K. Martin, M. Doyle, D. Murphy, S. Graham, C. E. Newman, S. Bell, C. Treloar, A. J. Browne, and P. Aggleton, "Beyond deficit: 'strengths-based approaches' in indigenous health research," *Sociology of Health & Illness*, vol. 43, no. 6, pp. 1405–1421, 2021.

[32] V. Villarroel, S. Bloxham, D. Bruna, C. Bruna, and C. Herrera-Seda, "Authentic assessment: creating a blueprint for course design," *Assessment & Evaluation in Higher Education*, vol. 43, no. 5, pp. 840–854, 2018.

[33] D. Boud and N. Falchikov, "Aligning assessment with long-term learning," *Assessment & Evaluation in Higher Education*, vol. 31, no. 4, pp. 399–413, 2006.