Scientific Research Publishing

Creative Education, 2020, 11, 2541-2558
https://www.scirp.org/journal/ce
ISSN Online: 2151-4771
ISSN Print: 2151-4755

Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities?

Stephanie M. Redman[1], Kate J. Yaxley[1], Keith F. Joiner[2]

[1]School of Engineering and Information Technology, University of New South Wales, Canberra, Australia
[2]Capability Systems Centre, University of New South Wales, Canberra, Australia
Email: k.joiner@adfa.edu.au

How to cite this paper: Redman, S. M., Yaxley, K. J., & Joiner, K. F. (2020). Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities? *Creative Education, 11,* 2541-2558.
https://doi.org/10.4236/ce.2020.1112187

Received: October 27, 2020
Accepted: December 6, 2020
Published: December 9, 2020

Abstract

Cyber has evolved in the Information Age to penetrate and threaten all aspects of society. Arguably, undergraduate education needs to prepare graduates for cyber security as it does in communication and logic. Yet, most universities are so far only including cyber security as a new discipline. One university in 2015 made cyber security a general education subject. This research reports that the university's first major curricular and pedagogical reform for the general cyber security subject to be more realisable and appreciated by students. It also exemplifies the importance of well-designed laboratories for student appreciation and understanding within this new field and thus within educational research.

Keywords

Undergraduate General Education, Cyber Security, Reinforcement Laboratory Learning, Curriculum Reform, Contextualisation

1. Introduction

Cyber threats are becoming a pre-eminent concern within international affairs now that cyberspace is considered a natural condition for survival within modern developed societies (Kello, 2018). Cyber threat development is accelerating at such a rate (Chan, 2018) that there is a significant concern that a real-world attack could cause damage to the global dynamic (Austin, 2019; Ikeda et al., 2019). There is currently a lack of proactive development of cyber defence capabilities, focusing on reactive responses to threats (Mirkovic et al., 2010; United States Government Accountability Office, 2018). The eight vectors of cyber-attack and cyber defence include people and their education and awareness (Austin, 2016). By supporting cyber education, universities can combat ordinary user behaviour that otherwise makes them an attractive target for skilful cybercriminals (Yan et al., 2018). Preventative general education is either lagging or non-existent with a global "cyber security skills and education crisis" where Australia's cyberspace education sector is currently in its "infancy" (Henry, 2017). In the US, military universities have led the development of comprehensive cyber security education, with Hall & Sobiesk (2017) noting:

> *Few institutions require cyber security as part of their general education program. Examples of such requirements include mandated general education subjects at the United States Military Academy* (*Sobiesk* et al., 2015) *and the United States Naval Academy* (*Brown* et al., 2012). [*p.* 4]

According to Henry (2017), "Australian *universities should work with industry and government to ensure that cyber security programs are more directly preparing students for the workforce*." The most rudimental insurance measure to protect national cyber security is education (Kumar & Shah, 2014).

A search of educational research journals was conducted, excluding those journals particular to Information Technology and Computer Science programs. The investigation found documented curricular pressure only in business and entrepreneurship programs (Raineri & Fudge, 2019; Weiser & Conn, 2017). To illustrate the relatively low coverage for cyber security education, Chen et al. (2020) examined all 3963 articles in a leading educational research journal of long-standing, finding cyber security aligned with hardware discussion and that this was in "*continually decreasing research interest since earlier years*." By not investing in cyber security educational research, universities are risking the ability to graduate professionals capable of meeting the identified gap of cyber security professionals within Australia (Australian Computing Academy, 2019; Caelli, 2021), and broader industry (Caldwell, 2013), and further perpetuating the low maturity of cyber education (Austin, 2021).

In the above context, it is significant that in 2015 the University of New South Wales developed a baseline cyber security subject mandatory for all undergraduate students across all curriculums, meeting the realisation that cyber security exists beyond the specialist departments (Martin & Collier, 2021). The questions of all undergraduate universities are:

- Should there be a general cyber security education in undergraduate degrees?
- How should the content of general cyber security education be focused?
- What pedagogies make cyber security general education subjects realisable and appreciated by students and employers?

This research was primarily conducted to review the general cyber security subject content's alignment to the most applicable cyber security frameworks and to examine and improve the student realisation and appreciation of cyber security. In particular, teachers sought to develop and implement better practical reinforcement laboratories for improved understanding through better integrating practice, content, logical reasoning, and interpretation (Mouheb et al., 2019;

Tekkumru-Kisa et al., 2015). The key curricular aim was to focus the laboratory on topics that were more relatable for students, as such to build epistemological bridges from what they know to what they are learning (i.e., Constructivist) (Forero, 2016; Kretchman-Grande, 2018). This approach was also to recognise the diversity of students. The main pedagogical aim was to create appropriate opportunities for students to discuss cyber security in these laboratories and derive more robust and retained knowledge (i.e., Vygotskian (Vygotsky, 1978) or Connectivism). Such pedagogical objective derives from somewhat rare educational research on laboratories like Nickerson et al. (2007), who noted "the possibility that the lab's underlying technology might be less important than the discussion about the lab among the students."

The importance of this work lies in the paucity of cyber security skills in professionals (Henry, 2017; Yan et al., 2018). Suppose universities recognise a need to provide these skills. In that case, the hard-earned curricular and pedagogical improvements of a university with a general education in cyber security could improve the speed and effectiveness of such programs. This research also has educational policy implications across all universities to answer the three dot-point questions posed above in preparing emerging professional leaders for the new Synthetical Age (Reay-Atkinson et al., 2016; Preston, 2018). Finally, there is significance in this work on improving laboratories and focusing their continued use in new fields and contexts, addressing an apparent decline in educational research in this area (Chen et al., 2020; Nickerson et al., 2007).

2. Literature Review

To ensure our improved laboratory pedagogy met the industry's multidisciplinary needs, we consulted the Cyber Security Curriculum (CSC) (Association for Computing Machinery, 2017). We used the National Initiative for Cyber security Education (NICE) Frameworks (Newhouse et al., 2017) to identify relevant Knowledge, Skills, and Abilities (KSA) expected of students of Post-Secondary Degree Programs in cyber security. Those pertinent to the laboratory development are information storage security, data integrity, and secure communications.

With the complexities surrounding cyber security increasing significantly, there is heightened importance to maintain a progressive educational program to safeguard security at every level (Australian Signals Directorate, 2019). A fundamental principle of cyber security is that everyone secures it—meaning all cyber users are responsible for maintaining a high level of awareness against compromise (Hanson & Uren, 2018). Key concepts to be learned and reinforced are vulnerability analysis (VA) and the Common Vulnerability Scoring System (CVSS) (First.org, 2019; Mell et al., 2006). The Australian Defence Force (ADF) also identifies two key modules that constitute cyber security: passive and self-defence (Hansen & Uren, 2019). Active defence and offence compose the cyber operations sector, which is only legal by the Australian Signals Directorate (ASD)

(Slocombe, 2018). This difference is evident in **Figure 1**, highlighting everyone's importance for self-defence—verifying the awareness and safety components and passive defence to educate the laymen.

Three common cyber security education approaches are simulation-based environments (Gestwicki & Stumbaugh, 2015; Nicholson et al., 2016), the notion of collaborative learning using cyber competition (Bishop, 2018; Hall & Sobiesk, 2017), and cyber table-topping (Christensen, 2017; Lantto et al., 2019). Teaching cyber security with a collaborative model using a competition known as making the flag (MTF) has been successful (Bishop, 2018; Hall & Sobiesk, 2017). This exercise's drawback is that MTF assumes a high technical knowledge amongst participants and maybe beyond students who are not confident in technical situations. An option considered was to use forced heterogeneous group learning among technical and non-technical students seeking to foster an environment of student support and confidence between them; however, this mixed-ability in a competitive environment can risk tensions (Springer et al., 1999). The MTF approach was deemed too specialised for the general education subject of this research.

Lantto et al. (2019) researched the learning effectiveness of CTT exercises using a multi-team method on both closed and open networks because such CTT exercises are crucial to Government departments (Christensen, 2017) and industry (Dewey, 2017; Grance et al., 2006). Their research is not intended to suggest a model; instead, verify the need for CTT exercises in learning. They propose implementing a CTT exercise to identify differences in resilience while representing the most authentic simulated environment. Using Bloom's revised taxonomy (Krathwohl, 2002), Forero (2016) developed a framework adapted into student practical learning, centred on CTT. His framework aligns with the cyber curriculum and especially the learning objectives. While not applied directly, his teaching method exhibited epistemological scaffolding that could assist students in their overall conceptual understanding. Accordingly, this method was influential in the laboratory design to help students understand several concepts.

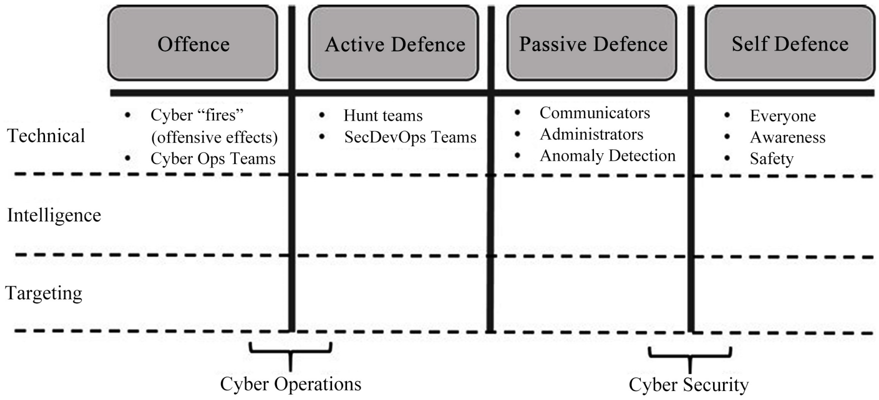

Figure 1. Framework for ADF Cyber Security operations (adapted from (Hanson & Uren, 2018)).

While many institutions offer introductory cyber security courses, very few provide an applied technical or laboratory component with no prerequisite knowledge. An exception was the University of Newcastle, which until recently offered a free short course to enrolled students and the general public on cyber security involving seven laboratory exercises to reinforce learning (OzBargain, 2019). Unfortunately, this free course's online and self-paced nature means the extent of student success is not known. Ideally, the cyber security competency assessments developed by Yan et al. (2018) would be conducted at the outset and end of such cyber security education subjects to measure their efficacy.

In summary, there is generally an absence of cross-subject studies in introductory-level cyber security. This research offered the opportunity to develop a laboratory program directed at undergraduate students with no prior experience to achieve a higher student appreciation level. The literature supports laboratories that combine collaborative learning with a scenario-based analysis, followed by a CTT exercise reinforcement.

3. Methodology and Development

The research focused on developing an executable laboratory for the University of New South Wales undergraduate subject "Introduction to Cyber Security," whose content aligns with the ADF cyber security and NICE frameworks. The subject educates around 160 students each semester to ensure all undergraduates complete the mandatory subject at some stage in their degree. Ethics approval was sought and granted to survey the students in a baseline and then experimental laboratory program across 2019.

Student surveys were constructed to measure the willingness and ability (Littlewood, 1996) of students in applying cyber security. Analysis of the results uses qualitative and quantitative methods, allowing teachers to understand the impact of subject diversity and new content on both willingness and ability. Students doing the cyber security laboratories in Semester One of 2019 were surveyed between weeks five and nine, first to gauge an understanding of how the initial subject content is appreciated and second to develop a baseline for later experimentation. These surveys focused on content, delivery, and assessment and primarily measured how reinforcing the baseline laboratories were to the lecturing. The survey responses were then analysed to identify and inform the shortfalls in student autonomy and necessary enhancements. Critical questions from all surveys are given just once in later figures in the results section. Similarly, descriptions of the initial and new laboratory programs are provided in the results section. The subject and laboratory component were also mapped to the ADF cyber security and NICE frameworks to identify any content concerns.

A plan for revised content and delivery options was developed to align with all stakeholders' desired outcomes. All aspects of the revised laboratories were designed to aid students in their experience, including the class content, lab scripts, technical/virtual environment, and resources. The delivery method had to appeal to all technical abilities without disengaging or disheartening students, so the laboratories remained on virtual machines in a closed environment. These virtual machines also meant the laboratories would stay safe and legal for the capstone CTT exercise to occur.

After development, the revised or experimental laboratory program was tested and implemented. Testing began in isolation by the developers working from start to finish before being implemented into the Semester Two subject as an early formative assessment, followed by the unmodified and summative laboratories. The precautions of trialling the new laboratories in a formative and duplicating experience were to ensure they were validated before replacing the baseline laboratories from Semester One in 2020. The revised laboratories' formative trialling occurred during weeks four to seven of Semester Two, a little early relative to the ideal in the lecture program. Student responses from the trial concerning alignment are likely to be somewhat affected, but this should be conservative compared to the baseline.

For the trial, two surveys were conducted to assess the suitability and draw conclusions on whether the revised laboratories are an improvement to the baseline, one before the lab beginning to assess student willingness, expectations, and baseline ability, and one upon completion to evaluate and compare student learning and appreciation. The pre-laboratory survey consisted of nine items with eight Likert-based questions and an open-ended and free-form question. In contrast, the post-laboratory survey was identical to that used on the baseline laboratories. Comparisons were drawn between the proposed and current programs to observe differences in student willingness, ability, and learning experiences. This information informed further improvements, refinements, and recommendations made to the subject for full implementation in 2020.

3.1. Baseline Subject Findings

Baseline surveys collected 158 anonymous students' responses, each coded and analysed using software packages NVivo (Qualitative) and Tableau (Quantitative). The coding was overseen by a second researcher but not independently verified, primarily because the findings were found to be clear and the changes sought were not controversial. The composition of the subject responses was approximately 16% Arts, 20% Business, 14% Science, and 50% Engineering/IT. The results suggest that most students agree that the cyber security laboratories are valuable and that some agree they have a better understanding of cyber security afterwards. There was less confidence amongst the Art students regarding protecting themselves against vulnerabilities compared to other disciplines. The final survey question substantiated the previously unverified hypothesis that the subject's technical component is less enjoyable to students from the less technical degrees, with decreasing enjoyment in order of decreasing technical content in degree programs.

In responses to the questions "*I have a better understanding of the importance* *of cyber security now*" and "*I have a better idea of how to protect myself against weakness/vulnerabilities*," shown in **Figure 2**, 19% and 42% of all student responses respectively were either neutral or negative. Hence following the baseline laboratory exercises, significant proportions of students still do not possess the confidence to ensure their security. Reinforcing a lack of penetration in the baseline subject, 14% of students responded in the negative when asked if they enjoyed the laboratory program overall.

Regardless of subject diversity, the current laboratory program did not support students' willingness (enjoyment) or ability (confidence).

Free-form and open-ended survey questions were analysed qualitatively. The critical theme discerned across degree streams was "*the excessive speed at which the content is delivered*." This finding suggests, supported by observations, that the students cannot keep up with the content due to its technical content and that the subject is not aimed at an appropriate introductory level. To further substantiate this, when analysing the responses for all degree streams using a word frequency search for the terms related to *complex*, *rushed*, or *too much content*, NVivo located 147 references in 87 of the 122 responses to the free-form question. Hence over half of the students had directly commented on these concepts. Superficially, there appeared to be a subject bias towards technical students; however, the comments received from the open-ended results showed that the students studying more technical disciplines are also facing the same time and complexity challenges as the less technical students. As such, these difficulties impact on the overall willingness and ability of all students.

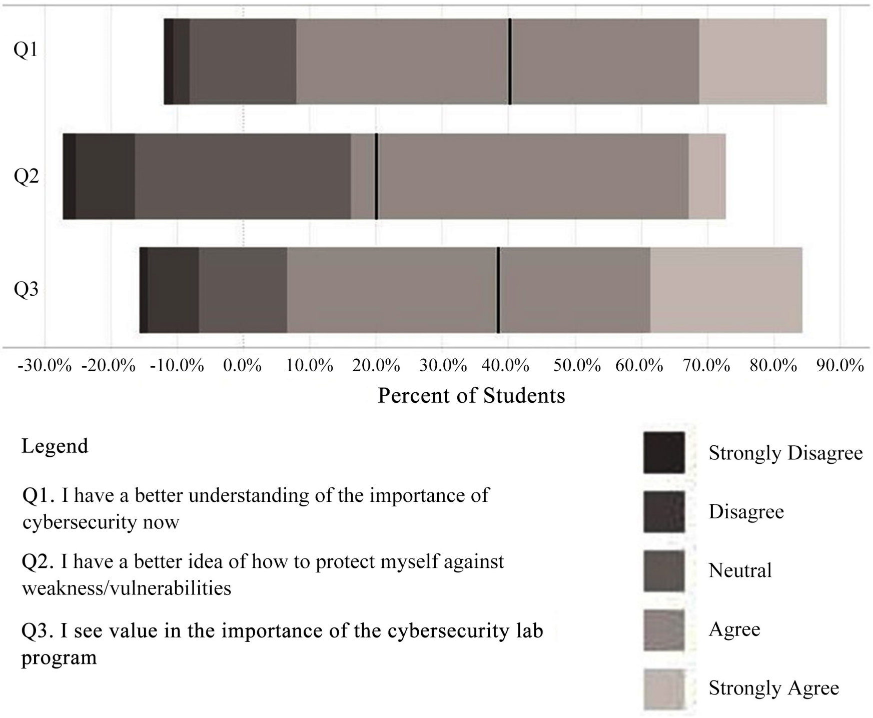

Figure 2. Survey responses of students to the baseline laboratory program (grouped).

3.2. Mapping Content with Frameworks and Subject Outline

The original laboratories span over nine weeks and cover the topics described in **Table 1**; they are conducted in two parts: an initial lecture and then a practical component (from observation). From the student surveys, there were a few responses regarding how lectures felt *impractical in a laboratory setting* (paraphrased) and that 50% of students thought they would have had a better understanding if the technical lectures and the laboratories were better aligned. While the topics covered in the current lab are imperative for building overall awareness and understanding of how vulnerable a system may be, it is essential to distinctly define the most effective learning method to achieve the required level of awareness. In some instances, the lecture content may be enough. In others, a demonstration may be more suitable (for example, how simple some malicious actions can be), leaving the practical applications to draw on multiple topics in an applied matter.

Some inconsistency was found in the mapping about the laboratories' description of what was executed with excessive amounts of technical content upfront. An example was the first introduction lecture contains 30 new concepts and associated acronyms. There are substantially more lectures than laboratories, and 16 student responses in the baseline mentioned the difficulty in keeping up. Therefore, a concern to address in the laboratory re-design was giving students more opportunities to "*reinforce theoretical teachings*" in a "*hands-on*" way.

The mapping also found a few concerns regarding what content constitutes an introductory subject of cyber security that is focused on self-defence and what crosses the line into cyber-operations (**Figure 1**). Specifically, the applied techniques of "*capturing network traffic*," "*exploiting targets*," and "*web site attacks*" (baseline laboratories 3, 5 & 6) appear to be passive and active defence more suited to building awareness in a lecture or demonstration environment.

The Cyber Security Curriculum recognises that there is assumed foundational understanding that underpins overall knowledge, such as an assumed technological literacy level (Association for Computing Machinery, 2017). For the subject's demographics, this assumption needs to be addressed to the lower levels of competency to include all subject participants. Furthermore, the Cyber Security Curriculum recommends that a disciplinary lens be applied to cyber teachings. This lens drives the approach and depth of content required to achieve the learning outcomes (Association for Computing Machinery, 2017). Given the diverse programs the students study, the researchers shifted laboratory focus to cover the basics, where students apply, analyse, and evaluate personal cyber security—per the third, fourth and fifth levels of Bloom's taxonomy (Bloom, 1956; Krathwohl, 2002).

The subject content mapping also analysed the roles required for future Defence leaders studying at the University of New South Wales to communicate and understand cyber security against the KSA competencies of the NICE framework. Those jobs deemed important stepping-stones for emerging Defence

Table 1. Baseline laboratory topics.

Lab	Title	Lab	Title
1	Introduction	6	Using exploits to gain access to websites
2	OSI and Internet models	7	Social engineering
3	Reconnaissance and scanning	8	Wireless networks 1
4	Scanning and exploits	9	Wireless networks 2
5	Using Exploits to gain access		

leaders are categorised as, Leadership, Planner, and Management positions. More specifically, Executive Cyber Leadership, Cyber Policy and Strategy Planner, Authorising Official, and Program Manager are especially pertinent to ADF roles.

However, as introduced by the Cyber Security Curriculum, it is vital to cover knowledge areas and concepts through a wide range of disciplinary lenses firstly at a low level (Association for Computing Machinery, 2017). Using the NICE KSAs and the various lenses, a detailed formal laboratory script was developed to address and achieve the learning outcomes appropriately.

New laboratory program development maximises the quality of the time spent on the cyber range and allows time for collaborative learning. Researchers decided to limit the number of laboratories to three practical sessions. These sessions would focus primarily on personal security and encourage higher thinking into "*the internet of things*" to grow an abstracted awareness and understanding of the complexities of the cyberspace realm (Zhou et al., 2019). The final content of the three recommended laboratories is detailed in **Table 2**.

3.3. Pedagogy

Bishop (2018) chose a collaborative pedagogy to leverage work, where students get a more diverse experience and exposure to cyber security. Student responses from the baseline survey indicated that when they could not keep up, they became disengaged (lost willingness) and failed to complete the laboratories (ability not fostered). By encouraging group-work and modelling the proposed lab about a collaborative approach, students can draw on each other's strengths to bridge the technical gap and exchange thoughts and opinions through conversation. Utilising this approach aims to assist students who have little technical computer skill while promoting discussion to increase students learning through other perspectives (Nickerson et al., 2007; Springer et al., 1999; Vygotsky, 1978) and ultimately increase cyber security awareness (Yan et al., 2018).

3.4. Laboratory Content

As previously outlined, students used existing virtual machines on the cyber-range to encourage a safe and isolated environment for students to grow their skills and awareness of vulnerabilities without posing a risk to their private devices. Using virtual machines allows for employing a familiar configuration to students and exposing them to attacking mechanisms. Three virtual machines were used for the new laboratories, two replicate a Windows 10 machine, mimicking a personal device, and one Kali machine representing the attacker's device. Each of the individual machines contains programs, applications, or vulnerabilities that, if susceptible, can be exploited per the details in **Table 3**.

Lab 1-Image 1 is intentionally more vulnerable to show the effects and numerous methods whereby a machine can be compromised. Then, six low-level attacks were introduced and executed by students, as presented in **Table 4**. These attacks have been designed in such a way that is executed and undetectable on Lab 1-Image 1. Most will be detected in Lab 2-Image 2. The purpose of this second configuration is to have students understand, apply, and analyse personal cyber security—Bloom's second, third, and fourth levels (Bloom, 1956; Krathwohl, 2002). In these stages, it allows students to observe the simplicity and effects of a compromise on Image 1 (understand), to then rank the threat each vulnerability poses (apply), as well as theorise methods of mitigation (analyse). The same attacks are then executed on a secure system (Lab 2-Image 2) where observations and conclusions of the differences between machines can be drawn. Additionally, this exercise exhibits the strengths and weaknesses of different antivirus software, with Defender showing no threats detected while FortiClient detects most; however, not all; proving even an effective antivirus is not an entirely protective solution.

Table 2. Revised laboratory program description.

Lab	Title	Description
1	Familiarisation and Attack	• Understand the basics of the system through task manager, command prompts, and antivirus (AV) • Using a vulnerable machine, choose three attacks, exploiting them, and ranking them using CVSS 2.0, and running an AV scan and observing what it does/does not catch
2	Understanding Mitigation	Using the updated machine to: exploit the same three attacks, run an Antivirus scan and observe what it does/does not catch.
3	Abstracting Concepts	CTT exercise: given an abstract scenario, identify three threats and appropriate mitigation for each.

Table 3. Virtual machine configuration.

System	Lab 1-Image 1	Lab 2-Image 2
Windows 10 Pro	1503	1903
Office	2010	2016
Windows SMB	Version 1	Version 3
System Defence	Defender (Windows)	FortiClient
VLC (video player)	Version 0.08	Version 3.01
Beef console	Microsoft Edge, Explorer, Chrome, Firefox, Opera	Microsoft Edge, Explorer, Chrome, Firefox, Opera

Table 4. Exploit descriptions.

No.	Vulnerable System	Attack type/Execution
1	Window 10	Baiting—Local attack using compromised USB, targeting human error
2	Microsoft Office—Macro	Social Engineering—Macro attack, establish a connection with the computer from a target machine
3	Microsoft Office—Application	Social Engineering—Vulnerable application attack through email
4	Human error/Outlook	Link within a link—Hidden URLs or hyperlink
5	Human error/Browser	Drive-by website—Browser manipulation
6	Wi-Fi	Drive-by Wi-Fi—Establish Kali machine connection.

3.5. Culminating Exercise

The final exercise draws specifically on group discussion around a CTT exercise. This exercise has students evaluate the cyber posture of an abstract item/environment using the knowledge, understanding, and skills obtained in the prior two labs and the remainder of the subject—addressing Bloom's fifth level (Bloom, 1956; Krathwohl, 2002). This exercise is conducted using a magnetic representation of the environment on a whiteboard, allowing students to interact and visualise the scenario physically. The scenarios vary from utilising a digital assistant in a sensitive location to an outdated organisation, each posing new and different challenges to digest. This exercise aims to synthesise their understanding by identifying vulnerabilities and mitigation strategies to provide recommendations, improving the cyber posture of the system at hand. Further, the task has students deal with abstracted cyber security flows in typical cyber security "*bow-tie diagram*" constructs (CGE Risk Solutions Ltd., 2019) commonly used in government or industry (Fowler & Sitnikova, 2019).

3.6. Learning Resources

The laboratory scripts, virtual machines, CTT exercise scenarios, and slides were developed with the laboratory demonstrator. These resources were reviewed and refined continuously throughout the development process to ensure they were suitable for students to follow along, with minimal reliance on the instructor, allowing the instructor to engage as much as possible with students throughout the laboratory in a Vygotskian style of pedagogy (Udvari-Solner & Thousand, 1996). The scripts were used as the primary resource for students during the laboratories, and hence they needed to be detailed and unambiguous.

4. Findings

The pre-laboratory survey had 123 responses with a subject composition of 24% Engineering or IT, 41% Arts, 16% Business, and 19% Science. Shown in **Figure 3** are appreciation pre-lab survey responses. The demographic has less Arts students than the baseline, which was expected due to the program schedule. From the Likert questions, the categorisation results closely align with the preliminary investigation, where positive responses favour the more technical students. Furthermore, all degree streams returned almost identical distribution when asked if they had any idea how to protect themselves, constituting roughly a 50% split on both positive and negative responses for all. Consequently, there is generally an overall willingness and understanding of the laboratories' importance amongst all degrees.

When analysing the data from the question, "*The thing I am most looking forward to learning at the cyber security labs is*, *and why*," the key theme was a desire for practical applications where the students can extend their technical skill to protect themselves (improving ability). This sentiment aligns with results obtained from a similar question in the baseline survey ("*What was your favourite part of the cyber labs*?").

After the trial of new laboratories, all students were again invited to survey the subject in the same format utilised in the preliminary investigation, with 75 responses collected. The demographic was: 17% Engineering/IT, 32% Arts, 6% Business, and 20% Science. In the quantitative Likert-data, responses are more favourable compared to the baseline laboratories. The appreciation responses in Figure 4 have increased for two of the questions, with only 13% and 8% neutral and no negative responses compared to 20% and 42% negative respectively in the baseline laboratories. These results indicate that the proposed laboratory program evokes significantly more confidence (improved ability) in all students regardless of degree stream, ensuring they are more likely to address and protect themselves. Furthermore, student willingness improved to only 17% of students recording negative or neutral responses, reducing from 44% in the baseline laboratories.

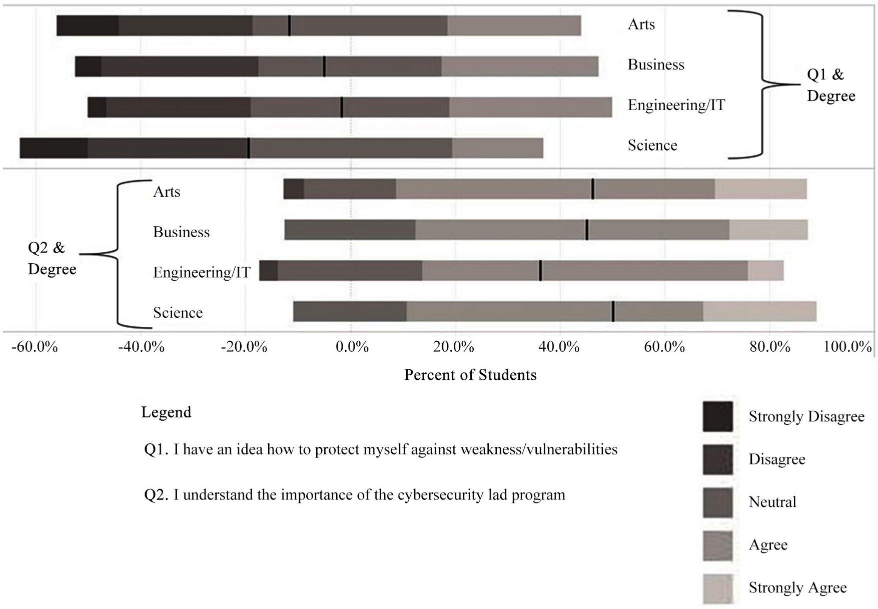

Figure 3. Appreciation pre-lab survey responses.

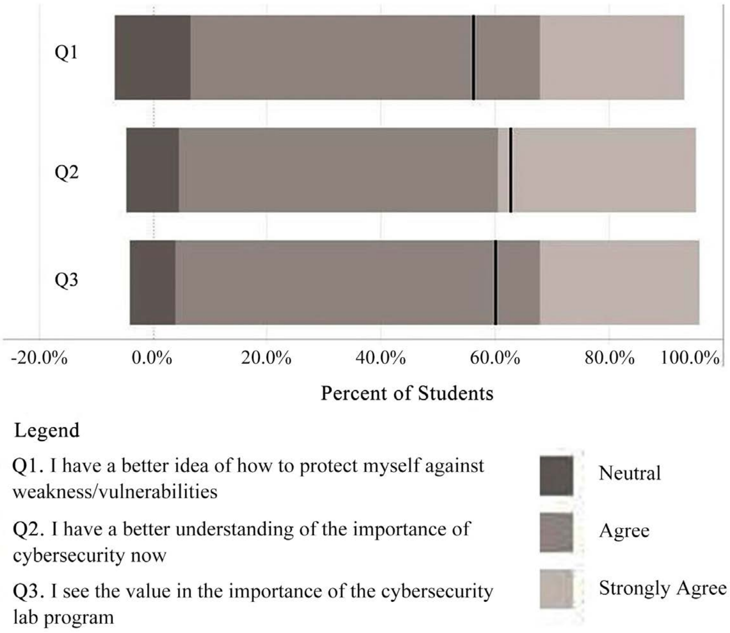

Figure 4. Appreciation pos-lab survey responses (grouped).

From the open-ended questions, student concern sentiments have shifted from content and delivery to instruction; "*If there was one thing that you would change for the cyber labs, what would it be*," where better instruction or direction was a shared concern. This concern can be addressed in further iterations through pedagogy. Additionally, using the same word frequency search as the preliminary investigation, 17 of the 63 responses; 27% stated their least favourite part of the lab was that they were complex, rushed, or had too much content, down from 71% in the baseline laboratories.

5. Discussion

Evidence that undergraduate general education in cyber security is necessary and relevant has been found by (Yan et al., 2018) and reinforced by the University of New South Wales experience and this research. Furthermore, programs for specialist cyber security education have been well documented (Association for Computing Machinery, 2017; Newhouse et al., 2017); albeit, their penetration and consistency in places like Australia are still mostly inadequate (Australian Computing Academy, 2019; Henry, 2017). The primary education gap is in the development and efficacy of general cyber security education of the type called for by Yan et al. (2018) and developed in this research. Unfortunately, a major limitation of the research here is that it was focused mainly on student satisfaction and willingness and had no standardised metrics of competency. The tasks developed by Yan et al. (2018) should ideally be standardised and used before and after, or with and without, the laboratory programs designed in this research, to establish a standard measure of the efficacy of this, and indeed other pedagogical initiatives aimed at filling this urgent educational need. Another future work would be to examine graduates of this university's program longitudinally for whether their appreciation changes in their industry roles, and they reflect different needs to those provided by this curriculum initiative. Given the diversity of such job roles across the industry, any such study would need to apply a careful Pareto approach (Newman, 2005).

6. Conclusion

The world of cyber security is ever-evolving, increasing the need for a baseline level of cross-disciplinary education. To achieve this baseline understanding, the Australian Government (Australian Signals Directorate, 2019) recommends everyone invests in developing an overall awareness of cyber security. The University of New South Wales took the first steps in 2015, offering a compulsory subject to all undergraduates, providing them with an opportunity to develop theoretically and applied foundational knowledge. A content review of this general education in cyber security against new cyber security education frameworks has created a better alignment of the subject content with personal student defence, with better contextualisation and concept bridging for more advanced cyber-threat work later.

The pedagogical research focused on the laboratories and their aim to "*reinforce theoretical teaching by providing practical hands-on sessions in a controlled environment*." Evaluation of baseline laboratories found this outcome had been challenged because many students struggled to remain engaged and found the labs were pitched at a high-level. However, by applying proven teaching methods, following internationally recognised frameworks and recommendations, a revised laboratory program of an appropriate technical level was developed. This laboratory improved the student willingness and ability from 44% dissatisfaction and 42% unconfident to 8% and 17%, respectively. By aligning the content to be focused more on personal cyber security, students indicated they found the subject was more appropriately paced and were able to build confidence to address their private cyber security.

This research is significant given the limited research of this type found in the meta-analysis by Yan et al. (2018). Moreover, the research sets an example for all universities to determine if:

1) They should have general cyber security education in undergraduate degrees,

2) How the content of cyber security general education should be focused, and

3) What pedagogies make cyber security general education subjects realisable and appreciated by students and employers.

By offering general cyber security education, educators have the opportunity to prevent the weakest link in cyber security—ignorant human behaviour towards cyber security. For this reason, we assert improving general cyber security education is a responsibility for all universities.

Acknowledgements

The laboratory development would not have been possible without the expertise and skill of industry professional Roger Smith. This research was supported and approved by the University's Human Research Ethics Committee (Number HC190198) on 30 April 2019, and all conditions therein were complied with through this research.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Association for Computing Machinery (2017). *Cyber Security Curricula 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cyber Security.* https://europe.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Austin, G. (2016). *Australia Rearmed! Future Needs for CyberEnabled Warfare*. Sydney: Australian Center for Cyber Security, University of New South Wales. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/DISCUSSION%20PAPER%20AUSTRALIA%20REARMED.pdf

Austin, G. (2019). Civil Defence Gaps under Cyber Blitzkrieg. *International Conference, Research and Education for the Cyber Storm,* Canberra. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Cyber%20blitzkrieg%207%20Feb%202019%20CONF%20VERSION.pdf

Austin, G. (2021). Ch. 13: Twelve Dilemmas of Reform. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies* (pp. 208-219). London: Taylor & Francis. https://doi.org/10.4324/9780367822576-13

Australian Computing Academy (2019). *Australian First: Cyber Security to Be Taught in Classrooms from 2019: Education, Banking and Technology Sectors Collaborate to Deliver Critical Cyber Security Skills to Students.* https://news.nab.com.au/news_room_posts/australian-first-cyber-security-to-be-taught-in-classrooms-from-2019

Australian Signals Directorate (2019). *Australian Government Information Security Manual.* https://www.cyber.gov.au/ism

Bishop, M. (2018). A Design for a Collaborative Make-the-Flag Exercise: IFIP Advances in Information and Communication Technology. *IFIP World Conference on Information Security Education (WISE): Towards a Cybersecure Society.* https://doi.org/10.1007/978-3-319-99734-6_1

Bloom, B. S. (1956). *Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain*. Philadelphia, PA: David McKay Co. Inc.

Caelli, W. J. (2021). Ch 1: History and Philosophy of Cyber Security Education. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies* (pp. 8-28). London: Taylor & Francis. https://doi.org/10.4324/9780367822576-1

Caldwell, T. (2013). Plugging the Cyber-Security Skills Gap. *Computer Fraud & Security, 2013,* 5-10. https://doi.org/10.1016/S1361-3723(13)70062-9

CGE Risk Solutions Ltd. (2019). *How to Deal with Generic Threats like Cyber Attacks? BowTieXP Allows You to Understand and Manage Your Risks through Barrier Based Risk Management.* https://www.cgerisk.com/solutions/cyber-security

Chan, S. (2018). Prototype Orchestration Framework as a High Exposure Dimension Cyber Defense Accelerant amidst Ever-Increasing Cycles of Adaptation by Attackers: A Modified Deep Belief Network Accelerated by a Stacked Generative Adversarial Network for Enhanced Event Correlation. In: *CYBER 2018: The Third International Conference on Cyber-Technologies and Cyber-Systems* (pp. 28-38). Athens: IARIA.

Chen, X., Zou, D., Cheng, G., & Xie, H. (2020). Detecting Latent Topics and Trends in Educational Technologies over Four Decades Using Structural Topic Modeling: A Retrospective of All Volumes of Computer & Education. *Computers & Education, 151,* Article ID: 103855. https://doi.org/10.1016/j.compedu.2020.103855

Christensen, P. (2017). Cybersecurity Test and Evaluation: A Look Back, Some Lessons Learned, and a Look Forward! *ITEA Journal, 38,* 221-228.

Dewey, J. (2017). *Whiteboard Wednesday: Incident Response—Tabletop Exercises*. Rapid 7. https://www.rapid7.com/resources/wbw-incident-response-tabletop-exercises

First.org (2019). *Common Vulnerability Scoring System (CVSS-SIG).* https://www.first.org/cvss

Forero, C. A. M. (2016). *Tabletop Exercise for Cybersecurity Educational Training; Theoretical Grounding and Development*. MS Thesis, Tartu: University of Tartu. https://www.academia.edu/34091273/Tabletop_Exercise_For_Cybersecurity_Educational_Training_Theoretical_Grounding_And_Development

Fowler, S., & Sitnikova, E. (2019). Toward a Framework for Assessing the Cyber-Worthiness of Complex Mission Critical Systems. *Military Communications and Information Systems Conference (MilCIS),* Canberra, 1-6. https://doi.org/10.1109/MilCIS.2019.8930800

Gestwicki, P., & Stumbaugh, K. (2015). Observations and Opportunities in Cybersecurity Education Game Design. *2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES),* Louisville, 27-29 July 2015, 131-137. https://doi.org/10.1109/CGames.2015.7272970

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. Special Publication 800-84. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf https://doi.org/10.6028/NIST.SP.800-84

Hall, A. O., & Sobiesk, E. (2017). Integration of the Cyber Domain at the United States Military Academy. *Proceedings of the International Workshops Realigning Cybersecurity Education,* Melbourne, 24 November 2017, Vol. 10, Article No. 3293881.3295778.

Hanson, F., & Uren, T. (2018). *Australia's Offensive Cyber Capability*. Canberra: Australian Strategic Policy Institute. https://www.aspi.org.au/report/australias-offensive-cyber-capability

Henry, A. P. (2017). *Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements*. Discussion Paper. https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/ACCS-Discussion-Paper-4-Web.pdf

Ikeda, K., Marshall, A., & Zaharchuk, D. (2019). Agility, Skills and Cybersecurity: Critical Drivers of Competitiveness in Times of Economic Uncertainty. *Strategy & Leadership, 47,* 40-48. https://doi.org/10.1108/SL-02-2019-0032

Kello, L. (2018). Cyber Threats. In T. G. Weiss, & S. Daws (Eds.), *The Oxford Handbook on the United Nations* (2nd ed.). Oxford: Oxford University Press.

Krathwohl, D. R. (2002). A Revision of Bloom's Taxonomy: An Overview. *Theory into Practice, 41,* 212-218. https://doi.org/10.1207/s15430421tip4104_2

Kretchman-Grande, J. (2018). *Re-Assessing Assessment: Implementing Constructivist Testing with New and Existing Curriculum* (p. 224). School of Education Student Capstone Projects. https://digitalcommons.hamline.edu/hse_cp/224

Kumar, A., & Shah, J. (2014). The Threat of Advancing Cyber Crimes in Organisations: Awareness and Preventions. *International Journal of Advanced Research in Computer Science, 5,* 85-89. http://search.proquest.com/docview/1658427294/?pq-origsite=primo

Lantto, H., Åkesson, B., Suojanen, M., Tuukkanen, T., Huopio, S., Nikkarila, J., & Ristolainen, M. (2019). Wargaming the Cyber Resilience of Structurally and Technologically Different Networks. *Security and Defence Quarterly, 24,* 51-64. https://doi.org/10.35467/sdq/103346

Littlewood, W. (1996). "Autonomy": An Anatomy and a Framework. *System (Linköping), 24,* 427-435. https://doi.org/10.1016/S0346-251X(96)00039-5

Martin, A., & Collier, J. (2021). Ch 3: Beyond Awareness: Reflections on Meeting the Inter-Disciplinary Cyber Skills Demand. In G. Austin (Ed.), *Cyber Security Education: Principles and Policies* (pp. 55-73). London: Taylor & Francis. https://doi.org/10.4324/9780367822576-3

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common Vulnerability Scoring System. *IEEE Security and Privacy Magazine, 4,* 85-89. https://doi.org/10.1109/MSP.2006.145

Mirkovic, J., Benzel, T. V., Faber, T., Braden, R., Wroclawski, J. T., & Schwab, S. (2010). The DETER Project: Advancing the Science of Cyber Security Experimentation and Test. *2010 IEEE International Conference on Technologies for Homeland Security,* Waltham, 8-10 November 2010, 1-7. https://doi.org/10.1109/THS.2010.5655108

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity Curriculum Design: A Survey. In Z. Pan, A. D. Cheok, W. Müller, M. Zhang, A. El Rhalibi, & K. Kifayat (Eds.), *Transactions on Edutainment XV* (pp. 93-107). Berlin: Springer. https://doi.org/10.1007/978-3-662-59351-6_9

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. *NIST Special Publication, 800,* 181.

Newman, M. E. (2005). Power Laws, Pareto Distributions and Zipf's Law. *Contemporary physics, 46,* 323-351. https://doi.org/10.1080/00107510500052444

Nickerson, J. V., Corter, J. E., Esche, S. K., & Chassapis, C. (2007). A Model for Evaluating the Effectiveness of Remote Engineering Laboratories and Simulations in Education. *Computers & Education, 49,* 708-725. https://doi.org/10.1016/j.compedu.2005.11.019

OzBargain (2019). *Free Course: Introduction to Cybersecurity from University of Newcastle*. OzBargain. https://www.ozbargain.com.au/node/434515

Preston, C. J. (2018). *The Synthetic Age: Out-Designing Evolution, Resurrecting Species, and Reengineering Our World*. Cambridge, MA: MIT Press. https://doi.org/10.7551/mitpress/11466.001.0001

Raineri, E., & Fudge, T. (2019). Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge within Top Universities' Entrepreneurship Programs. *Journal of Higher Education Theory and Practice, 19,* 73-92.
http://search.proquest.com/docview/2291990014
https://doi.org/10.33423/jhetp.v19i4.2203

Reay-Atkinson, S., Smallhorn, C., Caldwell, N. H. M., & Tolhurst, G. (2016). Identification and Classification—Designing and Engineering Synthetic Ecologies. *System Engineering, Test & Evaluation (SETE) Conference,* Melbourne, 128-142.

Slocombe, G. (2018). Cyber Security: Australian Signals Directorate (ASD) Is in the Defensive and Offensive Front-Line. *Asia-Pacific Defence Reporter, 44,* 34-36. https://asiapacificdefencereporter.com/australian-signals-directorate-asd-is-in-the-defensive-and-offensive-front-line

Springer, L., Stanne, M. E., & Donovan, S. S. (1999). Effects of Small-Group Learning on Undergraduates in Science, Mathematics, Engineering, and Technology: A Meta-Analysis. *Review of Educational Research, 69,* 21-51. https://doi.org/10.3102/00346543069001021

Tekkumru-Kisa, M., Stein, M. K., & Schunn, C. (2015). A Framework for Analysing Cognitive Demand and Content-Practices Integration: Task Analysis Guide in Science. *Journal of Research in Science Teaching, 52,* 659-685. https://doi.org/10.1002/tea.21208

Udvari-Solner, A., & Thousand, J. S. (1996). Creating a Responsive Curriculum for Inclusive Schools. *Remedial and Special Education, 17,* 182-192. https://doi.org/10.1177/074193259601700307

United States Government Accountability Office (2018). *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*. https://www.gao.gov/products/GAO-19-128

Vygotsky, L. S. (1978). *Mind in Society: The Development of Higher Psychological Processes*. Cambridge, MA: Harvard University Press.

Weiser, M., & Conn, C. (2017). Into the Breach: Integrating Cybersecurity into the Business Curriculum. *BizEd, 16,* 36-41.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? *Computers in Human Behavior, 84,* 375-382. https://doi.org/10.1016/j.chb.2018.02.019

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal, 6,* 1606-1616. https://doi.org/10.1109/JIOT.2018.2847733