Mastering the Cyber Security Skills Crisis:
Realigning Educational Outcomes to Industry Requirements

ACCS DISCUSSION PAPER NO. 4
Adam P. Henry
August 2017
Mastering the Cyber Security Skills Crisis:

Realigning Educational Outcomes to Industry Requirements

Adam P. Henry

ACCS DISCUSSION PAPER NO. 4
AUGUST 2017
Abstract

The cyber security skills crisis is a key policy issue in many countries, and governments look in part to universities to address it. This paper addresses one narrow question to see how it speaks to the broader challenges: are current Master of Cyber Security programs in Australia preparing students for the workforce? This research flags a new direction for further, much needed research rather than claim to be an exhaustive analysis. The paper outlines cyber security education as being multi-faceted and multidisciplinary and then identifies current gaps in university-based offerings. It pursues several lines of investigation. The first approach is to scope the field. To do that, and following a brief literature review, the paper proposes a new multi-level matrix, the Cyberspace Education Framework. This framework allows a high-level comprehensive view of cyberspace education. The paper then investigates current generalist master’s programs in Australia and the proposition that mission-specific and purpose-driven courses may better prepare students and address the skills crisis than generalist degrees. A survey of cyber security master’s students at one university campus and subsequent discussions with other stakeholders revealed a contrast between expectations. The paper then compares the current educational learning outcomes of Master’s programs in Australia with the knowledge, skills and abilities (KSA) set out in the U.S. Government’s work standards document as a proxy for what would be required for five cyber work roles of high national importance to Australia. It reveals only modest alignment (around 50 per cent) between the several Australian Master’s degrees reviewed and U.S. benchmark KSAs, compared with a 97 per cent alignment with them for a specialised Master’s degree at University College Dublin. UNSW Canberra does score a 77 per cent alignment for one U.S. identified role with one of its more specialised degrees, and Edith Cowan scores a 67 per cent alignment in the same role (cyber defence incident investigator). The paper concludes that the requirement for purpose-driven and mission-specific cyber security education is increasing and recommends that this become a focus of new initiatives in cyber security education. Universities have an obligation to work with industry and government to ensure that cyber security programs are more directly preparing students for the workforce. That will give Australia more chance to become cyber resilient and an opportunity to become a global leader in cyber security education.

ACCS Discussion Paper Series

The ACCS Discussion Paper Series is a vehicle to subject the research of scholars affiliated with the Centre to further review and debate prior to the finalisation of research findings in more formal scholarly outlets, such as journals or books. More information on ACCS is available at our website:

[https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/]
Table of Contents

1. Introduction................................................................................................................................. 1
2. Literature Review.......................................................................................................................... 2
3. Methodology.................................................................................................................................. 4
   3.1. Cyberspace Education Framework ....................................................................................... 5
4. Research Results.......................................................................................................................... 9
   4.1 Student Expectations Survey .................................................................................................. 9
   4.2 Industry Viewpoints ................................................................................................................ 10
   4.3 Educational Outcome to Work Role Comparison ..................................................................... 11
   4.4 Comparative View of Generalist versus Mission-specific Master’s Programs ..................... 12
   4.5 Framework Implications ........................................................................................................ 14
   4.6 Further Investigation with Informants .................................................................................... 14
5. Discussion...................................................................................................................................... 15
   5.1 Key Research Outcomes ........................................................................................................ 16
   5.2 Applying this Research .......................................................................................................... 17
   5.3 Areas for Future Research ..................................................................................................... 18
6. Conclusion...................................................................................................................................... 19
References......................................................................................................................................... 20
1. Introduction

The cyber security skills and education crisis is a key issue affecting countries globally. Governments are currently looking more and more to universities to help solve the problem. This paper looks at one key slice of the problem: are current Master of Cyber Security programs in Australia preparing students for the country’s workforce?

Cyber security education has become a new field of study across the world as a result of the rapid transformation of platforms, vulnerabilities and threats in the past decade. There is currently a lag effect between education research and the emerging needs in most countries. As governments release cyber security strategies, education is always mentioned, though, as cyberspace education is still in its infancy, there has been a certain lack of understanding of the field as a public policy problem and even as a pedagogic challenge (Austin, 2017). In the case of Australia, there is no single university scholar undertaking full time research into pedagogies and/or public policy for cyber security education. As Slay (2016) observed, there is a lack of people, there is no clear understanding of what cyber security means, what a cyber security professional is, or how they should be trained.

The Australian Cyber Security Growth Network’s Cyber Security Sector Competitiveness Plan (SCP) (2017, p. 2), states:

Australia has difficulty attracting and retaining cyber security talents. While the skills shortage is affecting the cyber security industry globally, there are signs that the lack of cyber talent in Australia is among the worst in the world. Australian firms struggle to find job-ready cyber security workers despite offering high wage premiums.

The government’s 2016 Cyber Security Strategy and the 2017 First Annual Update, report that ‘the scale and reach of malicious cyber activity affecting Australian public and private sector organisations and individuals is unprecedented’ (p. 2). These sentiments are supported by Austin (2016) and Austin and Slay (2016) which point out that while technical solutions are important, it will be institutional, cultural and social changes that will be most effective in mitigating cyber insecurity. New ways of thinking, new understanding and new strategies to the emerging digital age realities will be vital (Austin 2017, p. 1). As this field is complex and multidisciplinary, educational responses must focus not just on technical solutions but also incorporate the myriad of other topics such as national defence, economics, sociology, political science, diplomacy, history, and psychology (Kessler and Ramsay, 2013, p. 36).

Against this background, Australia’s cyberspace education sector is currently in its infancy. The Council of Australian Governments (COAG) in its December 2016 meeting identified cyber security education as an important area of future cooperation. As the 2016 Australian strategy and 2017 update concludes: ‘it is critical that we build our nation’s stock of cyber security skills, which are becoming increasingly essential for life and work in our connected world’ (p. 4). There is wide consensus that a considered multidisciplinary pedagogical focus appropriate to the more complex cyber threat scenarios affecting national public policy is required.
This paper argues for yet another step beyond recognition of the multi-disciplinary challenge. It argues for an approach that is not only multi-disciplinary but one that more explicitly recognises cyber security as comprising fundamentally distinctive specialisations at the outset, where different mission-specific sets (countering crime versus fighting cyber war, or child protection versus enterprise protection) define the learning objectives, the content, the level of expertise, and the value of various programs to future employers.

This sharpening of focus could then usefully be combined with mission-specific workplace integrated learning programs similar to those in medical education. But these workplace programs would not be for “general practice”. Currently, at the tertiary level at least, cyber security education prepares its graduates for some sort of general-practice, whereby courses cover the large base which is captured in the term cyber security. This may include network security, forensic studies, information assurance, programming and data analytics. Educational responses for cyber security may need to incorporate much earlier approaches that lie well outside the software and hardware aspects. In cyber security education policy and research on pedagogy, no convincing way has yet been found to incorporate the myriad of other topics (Cooper et al., 2010).

Cyber security should be viewed more like engineering with distinct differentiating sub-fields at a very early stage, such as electrical, mechanical, civil, aeronautical and bio-medical. A simple example that illustrates the intent of this paper is the proposition that the education needs for a person developing government policy on international cyber relations is very different to the education needs of a person working in a financial institution protecting their networks from cyber fraud. To extend the argument, neither of those professions requires any significant knowledge of cyber forensics on a scale that police authorities would need to be able to gain convictions for most forms of cybercrime.

2. Literature Review

There are few clear national visions and little consensus on how to solve the shortfalls in cyber security education and the subsequent skills crisis. In Australia, the Sector Competitiveness Plan supports this further by stating that there are signs the formal education system fails to produce enough job-ready cyber security graduates (Australian Cyber Security Growth Network, 2017, p. 35). The global cybersecurity skills gap has important implications and this has been widely acknowledged, but there is still the critical need to address the talent shortage by increasing the number of individuals who have cybersecurity skills (Vogel, 2016). This is compounded by a large amount of research focusing on the technologies and techniques of cyber security at the enterprise level, which contrasts with a distinct lack of research into cyber security education and pedagogical methods. There is some research into the field of system models for cyber security education in general terms, but it still does not quite go far enough. McGettrick (2013, p. 23) reiterates this point stating that cyber security is still an immature field lacking a cohesive intellectual body of activity and clear underlying science.

To ensure that cyber security education continues to mature Kessler and Ramsay (2013, p. 36), propose that academia needs to apply new ways of thinking, understanding, and strategies to a nation’s response to this new digital information age. This proposition aligns with the current emphasis on multidisciplinary approaches to cyber security education. Cyber security is about process as much as it is about technology, the response to cyber-related security challenges
today is not solely about technical solutions, but requires a multi-faceted and multidisciplinary focus (Kessler and Ramsay, 2013, p. 36).

There are currently few agreed metrics or baselines by which stakeholders can evaluate progress towards meeting the cyber security educational requirements. The United States has an overarching higher education mechanism with the Centres of Excellence and the models linking workforce needs to higher education outcomes (Conklin et al., 2014 and Kessler and Ramsay, 2013). There is also the newly announced Australian Government Academic Centres for Cyber Security Excellence (ACCSE), which aims to ‘increase the number of highly skilled post-graduates with the job ready skills needed to work in Australian business and government to tackle emerging cyber security challenges’. If universities do not adapt and modify their current methodology and course structure they will fall short, though it must be noted that the Australian government has not published any comprehensive baseline studies of the current outputs.

The key messages coming out of current research reiterates the importance of the purpose for the education (outlined below in the framework) and the importance of frameworks (models) for enhancing cyber security education and awareness (Amankwa et al., 2014, p. 250 and 2015, p. 76). Typically, these works offer a critical view of current curricula and the input/output method of education for cyber security which is universally seen as inadequate (Austin, 2017, p. 1; Conklin et al., 2014, p. 2008). There is a major gap in the alignment between the education of a student and the hands-on skills required to make them job ready. The central theme of this issue is training versus education. Training tends to be oriented towards the how and is focused on the current technology and methods. Education tends to focus on the why, the theory and mechanisms behind the professional activity. Linking theory and practice is vital for cohorts of Master of Cyber Security courses to be effective in the workforce. Cyber security is constantly evolving, making it challenging to acquire and maintain the skills necessary to act as a responsible cyber security professional (Martin, 2015).

This is not a new issue, as Hentea and Dhillon (2006, p. 226), observed a decade ago: ‘the adoption of courses that link theory and practice is vital for some courses offered for information security education, such that, the individual acquires the ability to put theories into practice’. There is a big discrepancy between the levels of skills expected by employers and those the graduates have after completing their studies. In order to address these problems, the academic community probably needs to restructure the curricula. Lehto (2016, p. 28) gives a grim view whereby universities only provide cyber security education from the university perspective. This is true for many universities, but there are some who are moving towards industry partnerships to enhance the effectiveness of their programs as a differential for potential students. This type of cooperation and collaboration is vital for the effectiveness of cyber security programs.

The key points that are necessary for cyber security courses to be relevant in the workplace are:

- depth over breadth (purpose driven) (Manson and Pike, 2014),
- work integrated placements (Koppi et al, 2008),
- practical skillset development - real world scenarios and simulations (kopi et al, 2010), and
The development of a single foundational curriculum that can meet all major requirements is not possible for a field as diverse as cyber security and thinking all graduates from all programs are interchangeable can be as bad in cyber security as any other specialised profession (Conklin et al, 2014). A key requirement for courses to remain relevant is to continually update the teaching and learning methods and ensure the content is in line with industries new direction. Koppi et al (2010), put forward that the relationship between industry and universities needs to be improved particularly with respect to the development of industry-integrated curricula. This requires an understanding of not only the purpose of the course for the university, but also the purpose and relevance to the student undertaking the course (Armstrong et al, 2013). High-quality cyber security programs need to differentiate between the multidisciplinary aspects of courses and the unique requirements for each course. A strong technical based curriculum requires hands-on activities including the use of cyber ranges, simulations and war-games. This approach with purpose designed workplace integrated learning strengthens the knowledge and skillsets of the students and improves employability. The Sector Competitiveness Plan supports this as globally with more than three-quarters (77 per cent) of cyber security professionals surveyed, think the industry's current training and education programs are not fully preparing professionals for the workplace reality. Leading to calls for academic programs to incorporate more practical learning. This hybrid technical cyber security education program should still be purpose-driven and mission-specific.

It should be noted that it is common practice in other academic programs to have a strong focus on practical skills acquired during work placements. A report into work experience in Australia stated that 71 percent of respondents were satisfied or very satisfied with the work experience and that they had developed relevant skills and knowledge. Nearly 30 percent of respondents were offered an employment opportunity after completing their placement (Australian Government Department of Employment, 2017). Koppi et al (2010) states that while fundamental theories were seen as providing a firm foundation for a dynamic and changing discipline, there is an unfulfilled need for their practical relevance and application to the real world. There will always be a challenge in academia to bridge the gap between theory and the real needs of industry. These performance measurements through real-world scenarios are critical in becoming effective in the workplace. This is prominent in the field of medicine. There are large components of workplace integrated learning in the medical field. This is also dependent on knowledge, skill levels and specialist training/ workplace development. Time spent on the task for which the person is being prepared is critical for success. For cyber security education especially in the technical areas, there should be a requirement for this type of complex practical tasking that requires a high degree of mastery to gain success (Manson and Pike, 2014).

3. Methodology

The paper begins with an original characterisation of education needs in cyber security according to five broad headings, each with distinct sub-sets. The paper then demonstrates the potential value of that original framework by analysing just one slice through more than several hundred possible combinations. That slice is based on tertiary education (Master’s level) as the departure point, suggesting that similar analyses could be undertaken for at least several other levels or types of education (discussed below). The investigation has been based primarily on a survey of Master’s students or recent graduates at the University of New South Wales Canberra. The data was then analysed in the context of other information about expectations of employers and universities in order to begin to identify gaps in the expectations of
stakeholders. To establish a clear opinion of current students, the survey explored their expectations regarding their different Master’s programs. Comparing the work roles of these students to individual courses taught in the Master’s programs also enabled gaps to be identified. Further to this, the Cyber Security Education Framework enables a clear and consistent comparison for the current offerings. Both international and national employer survey results were compared with the students’ opinions. Discussions with a recruitment firm were undertaken to ensure the results were consistent with current views in industry and with recommendations of the paper. Discussions with key personnel in several universities were also undertaken to explore the results and individual expectations of their courses.

3.1. Cyberspace Education Framework

This framework focuses on the broad high-level education objectives, which can then be narrowed down to show key outcomes for mission-specific activities. This approach reminds us that there can be no single universal approach to cyber security education. It is multi-faceted, multi-dimensional and purpose specific. At the same time, the framework allows us to see relationships between different education activities and outcomes. When it comes to baselines and benchmarks for cyber security education, it is a basic contention of this model, that these can only be established by reference to particular slices through this framework. The purpose of the framework reiterates the requirement for nations to pursue cyber education maturity (Austin, 2017). Within the framework five elements make up the matrix which leads to a very large number of quite distinct cyberspace education outcomes.

![Cyberspace Education Framework](image)

**Figure 1. The Cyberspace Education Framework**

**Education Type**

There are nine key categories of education type. This captures the different formal and informal types of education someone may pursue. This model identifies that an individual may undertake one or more different levels of education. The education undertaken is not defined by a sequence, but rather it is assumed that the education patterns undertaken differ from individual to individual and that each type can be undertaken more than once (that is, revisited).

The categories of education are:

- On the job training
Level of Expertise

The model proposes five key levels of expertise, but this is only a departure point. These range from Basic through to an Advanced Expert. The majority of formal courses available are within the basic through to expert levels. Each level of expertise needs to be viewed against each element of the framework as there are many different streams within cyberspace. Examples against each level are shown below in Table 1, while also reflecting the fundamental point that within even one level of cyberspace education there are multidisciplinary fields and purposes. Having technical expertise can be considered as important as having international relations expertise. While the two are very different fields of education and specialisation, both need to be ranked against the five levels of expertise.

<table>
<thead>
<tr>
<th>Level</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>A student within a primary school who completes a course regarding eSafety to a high standard; a CEO who knows cyber security is essential for profitability but does nothing about it; A criminal using stolen credit card details.</td>
</tr>
<tr>
<td>Intermediate</td>
<td>A Vocational Education and Training (VET) student who successfully completes a Certificate in Information Security; a lawyer who takes an effort to segregate sensitive data sets relating to an individual high value client; A criminal using phishing scams to capture people’s logon details.</td>
</tr>
<tr>
<td>Advanced</td>
<td>A PHD graduate specialising in system defence and cyber resilience for an organisation, whose research includes practical studies and scenario-related exercises; a graduate of several professional certifications (such as CISM, CISSP(^1)) who also has significant experience in threat mitigation and system resilience; an individual who develops ransomware and initiates major attacks for financial gain.</td>
</tr>
<tr>
<td>Expert</td>
<td>A cyber security professional has completed the Certified Cyber Security Expert (CSX) course offered by ISACA; an individual who through accessing third party vendors gains access to and steals intellectual property from a major multinational organisation for a nation state.</td>
</tr>
<tr>
<td>Advanced Expert</td>
<td>Certification as a Cyber Guardian offered by System Administration, Networking, and Security Institute (SANS). The institute has issued 86,900 certifications to computer professionals, of which only 35 are Guardians; Members of the teams who invented and evaluated the Stuxnet worm.</td>
</tr>
</tbody>
</table>

Table 1: Examples of Levels of Expertise

\(^1\) Certified Information Security Manager (CISM) is an industry certification offered by ISACA and Certified Information Systems Security Professional (CISSP) is an industry certification offered by (ISC)\(^2\).
Field of Education

The list below shows the broad fields of education in regard to cyberspace. It is important to note that only one field focuses on technical and this demonstrates the multidisciplinary nature of cyber security. Utilising this type of multidisciplinary model into the framework enables a broader view of cyberspace. This is a key aspect of the framework and the baselining process.

Five key fields of education:

- Political
- Social
- Legal
- Technical
- People

Purpose

To develop more effective and more focussed education policies, there is a requirement to address what specifically we need these skills for. Each country requires a cyber-educated workforce. This not just for national security agencies and police agencies, but all industries ensuring continued economic growth. It is therefore important within the framework to identify the reason or purpose (the mission set) for undertaking the cyberspace education.

The broad types of purpose (mission sets) are many, and this framework proposes 13 distinct mission sets:

- Espionage/counter espionage
- Counter-terrorism
- Countering crime (police)
- Cyber-enabled war
- Protection of the financial services sector
- Protection of other critical infrastructure
- Protection of children
- Intellectual property protection
- Privacy protection
- Legislation development and legal practice
- SME and Enterprise cyber security (resilience)
- Non-Government Organisations and political party cyber security
- Home user cyber security.

Application

We can also identify quite different aspects of cyber security education depending on the process the student will adopt to apply the knowledge/skills or the institutional circumstances. The broad types of application are listed below:

- Individual action
- Team member
- Team leader
The Cyberspace Education Framework enables comparisons between cyberspace education activities and what the outcome of each activity is. This framework helps establish baselines for future comparison. The results of the comparison show the effectiveness of the framework for cyberspace education policy development.

Matrix

These five elements, each with five or more distinct categories, allow us to postulate a very large number of education types and outcomes. While we may not expect all possible elements to be meaningful (e.g., primary school/advanced/technical/cyber war/team leader), the matrix allows us to understand the potential of much sharper focus. In particular, primary school children need to know child protection, before they need to know technical issues such as coding. The matrix also allows us to situate existing programs and align them with specialisations, mission sets, roles and outcomes. This is a very different approach to that of core competencies which has been a focus of much public policy discussion and which is important work. It is however far from being the whole story, and may not even be the main story. Table 2 brings together the sub-elements of each of the five main elements. The shaded sub-elements represent the “slice” of the education problem this paper is looking at.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>EXPERTISE</th>
<th>FIELD</th>
<th>PURPOSE</th>
<th>APPLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the job training; Self-Taught; Primary School; Secondary School; Vocational; Higher Education; Industry Certifications; Adult Education; University of the Third Age.</td>
<td>Basic; Intermediate; Advanced; Expert; Advanced expert.</td>
<td>Political; Social; Legal; Technical; People;</td>
<td>Generalist: Espionage/counter espionage; Counter-terrorism; Countering crime (police); Cyber-enabled war; Protection of the financial services sector; Protection of other critical infrastructure; Protection of children; Intellectual property protection; Privacy protection; Legislation development and legal practice; SME and Enterprise cyber security (resilience); Non-Government Organisations and political party cyber security; Home user cyber security.</td>
<td>Individual action; Team member; Team leader; Mid-level management; Executive management; National policy leadership (government or private sector); Community policy leadership.</td>
</tr>
</tbody>
</table>

Table 2. Matrix view of the Cyberspace Education Framework

It is against the consideration raised by elaborating the matrix, that the author believes we can better evaluate any existing programs. This paper chooses just one slice of the matrix Higher
education) and one subset of it (Master’s degrees) to understand better the state of cyber security education in Australia. This slice is marked in grey (yellow) shading in the above table. It is a basic corollary of the matrix that all slices need to be evaluated, in broad terms at least, against the criteria listed.

4. Research Results

To appropriately answer the question “are Master of Cyber Security programs preparing students for the workforce”, this project explored the viewpoints of students, employers and universities, comparing key data points and information to ensure a solid comparative base for the research. The 2016 NIST Framework2 of work roles in cyber security linking the knowledge, skills and abilities (KSA) to educational outputs also enables a further comparison between the current master’s programs and the top five skills crisis work role requirements. Further to this, the Cyberspace Education Framework was used to compare current generalist cyber security degrees to the more mission-specific Master of Science in Computer Forensics and Cybercrime Investigation course. To demonstrate how a mission specific program can more adequately address a specific industry requirement.

This holistic analysis provides a deeper view into the skills crisis and how universities can work towards ensuring their students are ready for the workplace.

4.1 Student Expectations Survey

The project surveyed current students and alumni of master’s programs at University of New South Wales (UNSW) Canberra. The campus has five master of cyber security offerings, mostly through distance learning, with some individual courses offered in one-week intensive mode on campus. The survey obtained responses from 22 percent of the 325 student cohort. Each course offered through the UNSW Canberra is represented in the survey but the majority of the cohort were undertaking Master of Cyber Security Operations (35 percent), Master of Cyber Security, Strategy and Diplomacy (28 percent) and Master of Cyber Security (24 percent). This demonstrates the multidisciplinary nature of the cyber security programs with students pursuing policy, international relations and strategy components as well as the traditional technical streams. 87 percent of the cohort were current students, with 93 percent of respondents studying in Australia.

There was a range of current occupations being undertaken by the cohort including a third from the Defence Force, 38 percent from private industry and 24 percent from state and federal public service. This reinforces the multi-faceted nature of cyber security and how broadly the requirements for a skilled workforce truly are. 56 percent of all participants were undertaking the course to gain a new role in a new workplace. 24 percent were undertaking the course to better equip them for their current position and 15 percent were undertaking the course as they were interested in the topic.

Interestingly 60 percent believe they will be able to utilise the knowledge and skillsets acquired in the course at their current workplace or appear to currently work in a cyber security role. A large portion (40 percent) do not work in the cyber security industry. 92.5 percent believe that

---

2 The U.S. Government National Institute of Standards and Technology (NIST) developed the Framework in response to Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which was issued in 2013. The Framework is voluntary guidance, based on existing standards, guidelines, and practices.
they would be able to utilise the knowledge and skillsets acquired in the course at a future workplace. 65 percent agreed that a work placement would be useful. 88 percent said that the course has given them further knowledge and skillsets they considered useful in either their existing workplace or future career goals. Of the 11.5 percent who said no, a large portion suggested that no practical skills or real world applications were taught. Of the 37 percent of students who had undertaken courses that provided cyber range simulations i.e. cyber operations including threat assessment, detection and prevention, 87.5 percent agreed that the simulations had strengthened their knowledge and skillsets for their future career ambitions. 83 percent of respondents rated the course satisfactory (slightly satisfied through to extremely satisfied) and was effective in meeting their expectations.

Interestingly 34 percent of respondents said they would undertake post graduate research, such as a Ph D and a further 45 percent would undertake an industry based certification. Three quarters of respondents had not undertaken an industry certification. Of the respondents who had undertaken an industry certification, 53 percent agree that they were effective in preparing them for their future ambitions and a further 42 percent neither agreed nor disagreed. The high rate of neither agree nor disagree could indicate respondents may have undertaken the course to fulfil a requirement for their resume.

These results show that a large portion of the cohort work in areas associated with cyber security, but a large number would be attempting to enter the cyber security workforce. The cohort is seeking new roles and has undertaken their course to improve their knowledge and skillsets. The high proportion of the cohort both supported the requirement for workplace integrated learning and the use of specific real world practical skills utilising scenarios and hands on labs.

4.2 Industry Viewpoints

In contrast to the student cohort there have been many surveys (national and international) conducted at the enterprise level regarding the skills crisis and skillsets required to fill cyber security positions. Recent studies by ISACA and the Australian Information Security Association (ASIA) reveal some interesting trends. The ISACA report stated that practical hands-on experience is the most important cyber security candidate qualification to 55 percent of enterprises. This is in stark contrast to formal education and personal endorsements ranked equally as least important (ISACA, 2017). This shows that current education and pedagogical methods aren’t hitting the mark. There is a high degree of focus on industry certifications with close to 70 percent of hiring enterprises requiring an industry security certification for positions.  This is in line with the findings of the AISA report, whereby many respondents did not think that current academic qualifications adequately prepared cyber security graduates for the workplace (AISA, 2017). The report states that experience is more important to recruiters than knowledge, certifications or education. It goes further to state that respondents were critical of the academic qualifications available for cyber security workers. Interestingly the report says that it may be because recruiters and employers do not understand the different academic qualifications that are available and the knowledge and capabilities of the graduates from those programs. As 40 percent of the student cohort surveyed aren’t currently in a cyber security role, they may have difficulty finding an appropriate position after their course.

This further demonstrates the requirement for courses to be aligned to workforce requirements. Universities should actively work with industry to ensure their programs are not only known to employers and recruiters, but relevant. An interesting trait the survey reported, was the
requirement for five years of experience with 90 percent of advertised cyber security positions (including junior positions such as security analysts) requiring this. The survey reported that architects, technical security consultants, forensic examiners, incident handlers or investigators and security analysts or advisors where the most in demand.

4.3 Educational Outcome to Work Role Comparison

The survey results indicate different expectations between students and employers and a low level of industry confidence in current programs. It is beneficial to compare how aligned current master’s program offerings are to the workplace KSA requirements, of the above most in demand roles to establish if there are major gaps or alignment. Using the NIST Framework for knowledge, skills and abilities related to work roles and comparing it to the units offered in the master’s programs establishes a clear picture of what industry has stipulated. This was done by comparing the course information provided on their websites to the KSA’s outlined in the NIST to create the matrix below (Table 3).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DEAKIN*</td>
<td>46%</td>
<td>32%</td>
<td>50%</td>
<td>47%</td>
<td>37%</td>
<td>97/225 (43%)</td>
</tr>
<tr>
<td>ECU*</td>
<td>43%</td>
<td>47%</td>
<td>67%</td>
<td>53%</td>
<td>37%</td>
<td>113/225 (50%)</td>
</tr>
<tr>
<td>UNSW Canberra</td>
<td>57%</td>
<td>58%</td>
<td>77%</td>
<td>57%</td>
<td>43%</td>
<td>131/225 (58%)</td>
</tr>
<tr>
<td>Total</td>
<td>79/162 (49%)</td>
<td>78/171 (46%)</td>
<td>58/90 (64%)</td>
<td>91/180 (51%)</td>
<td>35/90 (39%)</td>
<td>341/675 (51%)</td>
</tr>
</tbody>
</table>

Table 3. Generalist Course alignment to Work Role KSA

*It should be noted that Deakin University offers a unit specifically based on a Practical Project and Edith Cowen University offers a Work Integrated Learning unit which could increase their alignment with the work roles. These results offer a viewpoint into how the courses align and is offered for the purposes of discussion rather than as a definitive assessment. Future research could be undertaken to compare exact learning outcomes and criteria offered in the courses.

The total alignment of generalist master’s programs to work role KSA’s indicate an overall alignment of 51 percent. To accurately address the skills crisis, universities would need to amend their courses to better cover the required KSA’s. Currently all universities courses align the best with the Cyber Defence Incident Investigator work role. This could be a starting point for enabling greater consistency with work roles and actively working with industry further alignment. The Technical Security Consultant (Information Systems Security Operations) role was the most poorly aligned. This course could also benefit from industries input into core requirements and active internships/ work integrated learning opportunities. Universities could partner with consultancy organisations to provide options like an “earn and learn”, whereby students enter from a low level at the consultancy and as they develop and complete the course rise up the ranks. This would be useful for students who have no experience or a current role in cyber security. From these results it would be fair to say that the courses don’t currently align with the top five skills crisis work roles. This reinforces and supports the industry surveys results.
This demonstrates the requirement for developing the type of capability required for both students and employers requires new approaches focused on the growing and changing demands of the cyber security field.

4.4 Comparative view of generalist versus mission specific master’s programs

To put this into perspective this paper compares and contrasts three separate Master of Cyber Security courses (general practice) against a more mission-specific Master of Science - Forensic Computing and Cybercrime Investigation from University College Dublin, utilising the Cyberspace Education Framework. These courses provide a level of expertise within separate subsets of the cyber security field. The example looks at the generic cyber security (technical) degree compared to a mission-specific law enforcement focus specifically for law enforcement officers only. The example highlights the value of the mission-specific requirement for a degree when compared to the general practice Master’s degree. This focus enables a view of who must carry the responsibility for the specific purpose. In this example, it would be law enforcement agencies and governments appropriate policy areas for law enforcement, driving the course and providing relevant expertise and material. This could be at the state, national or international level. This mission-specific curriculum enables institutions to partner with relevant stakeholders and develop courses that fit a purpose or public policy requirement. Since we look to the private sector to provide relevant technologies and expertise to new cyber security education programs, we do need to note that private sector underpinnings of cyber-crime prevention are very different from those of other missions, such as cyber offensive and defensive operations for national security.

Table 4 below demonstrates how the mission specific education method compares to traditional curriculum.

<table>
<thead>
<tr>
<th>Education Type</th>
<th>Classic curriculum approach to Cyber Security (Technical) degrees</th>
<th>Master of Science - Forensic Computing and Cybercrime Investigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education Type</td>
<td>Tertiary (Post graduate)</td>
<td>Tertiary (Post graduate)</td>
</tr>
<tr>
<td>Level of Expertise</td>
<td>Intermediate</td>
<td>This depends largely on the specific institution and could only be considered at a higher level if they offer a hybrid model of learning including major work integrated learning opportunities and practical simulations utilising cyber-ranges.</td>
</tr>
<tr>
<td>Purpose</td>
<td>None of the key purposes on that axis of the matrix are specifically addressed by most master’s level cyber security programs. Most are designed to meet the demand for technical experts who can implement (not lead) low to mid-level technical cyber security functions “general practice” in government, industry or law enforcement.</td>
<td>Designed to meet only one purpose: Education and training for law enforcement officers in cyber-crime.</td>
</tr>
<tr>
<td>Objective</td>
<td>Each University states different objectives in a broad statement:</td>
<td></td>
</tr>
</tbody>
</table>

Table 4
Expert cyber security professionals who can protect organisations from these threats are in high demand and this course can prepare you for a successful career anywhere in the world (Deakin University).

It is designed for postgraduate scholars and professional managers with appropriate undergraduate qualifications in IT, computer science, electrical computer or systems engineering or a related discipline and/or extensive relevant professional experience who wish to gain a more detailed understanding of the technical skills and expertise relevant to the technical implementation and leadership of the cyber security function (UNSW).

This coursework degree is designed to meet the demand for cyber security professionals within government, law enforcement and industry. The course provides a pathway for existing information technology professionals seeking to commence or further progress their careers in the cyber security domain. It is also relevant to those seeking to enter the IT profession who have no previous experience in the cyber discipline (ECU).

Units of Study
- Computer Forensics
- Network Security
- Information Security
- Programming
- Project Management
- Wireless Security
- Data Analytics
- deliver cutting-edge, up-to-date cybercrime investigation techniques, strategies and tactics that allow students to understand and tackle emerging trends in cybercrime.

To teach existing law enforcement officials to be able to operate effectively and think critically in analysing and preforming cybercrime investigation through practical studies and scenario-related exercises to detect and secure prosecutions.

Units of Study
- Computer Forensics
- Network Investigations
- Malware Investigations
- Mobile Devices Investigation
- Linux for Investigators
- Live Data Forensics
- Data and Database Forensics
- Online Fraud Investigations
- Legislation
- Financial Fraud Investigation
- Case Study
- Research Project

Application

General Practitioner
Become a team member in a cyber-security team and enhance career with new workplace options operating within a range of often disconnected technical operations areas.

Law Enforcement Officer
Countering cyber-crime as an advanced technical specialist within a digital crimes law enforcement unit.

Table 4. Comparison of generalist to mission specific master’s course
(ECU, UNSW, DEAKIN, UCD, 2017)

It is interesting to note that all three Master of Cyber Security programs state law enforcement within the purpose. There are clear differences between the effectiveness and the knowledge/skillsets acquired from undertaking the general practice Master of Cyber Security compared to the Master of Science - Forensic Computing and Cybercrime Investigation. In performing the same analysis between the work role KSA’s for a Forensic Analyst to the learning outcomes of the UCD course, there was a 97 percent match between the educational outcomes and the work role KSA’s. This is a stark difference to the generalist courses. This clearly demonstrates the effectiveness and requirement for mission-specific cyber security education.
4.5 Framework Implications

The framework enables a high level comprehensive view of cyberspace education. This information is then collated to enable benchmarks and baselines to be developed into metrics. From this information, the purpose for the education can be identified. The purpose can also be identified as “the why”. Why is the education being undertaken or why is the education program being delivered? This is a very important aspect of the framework and goes towards successful educational policy and program development and implementation. This approach leads to purpose-driven or mission-specific education. For example, is a program being delivered to teach students about national security, create base-level enterprise security officers or just because cyber security seems popular at the moment.

The education outcomes need to be purpose driven, not driven by institutions that may not have any tangible links to relevant workplaces. Institutions aren’t the only piece in the puzzle, the same way governments/industry are not and neither can solve all the cyber security educational requirements. It is broad and requires multiple stakeholders working together. A purpose-driven focus enables stakeholders to look at the why and from that develop appropriate solutions i.e. new curricula for Master of Cyber Security. Updating and realigning the general practice approach with a more mission-specific purpose-driven method integrating workplace integrated learning and engaging with industry to optimise the master’s programs.

Having a course specifically for students who are already in law enforcement, enables students to apply their learning straight away. They are not required to undertake basic investigative or evidence gathering courses as that knowledge has already been acquired. This enables the course to be more in-depth and focused on more expert level outcomes.

Many governments try to initiate a single curriculum to solve the cyber security and/or skills crisis issue. This approach probably will fall short, as discussed above, the multidisciplinary nature of cyber security would require multiple different streams. While this is a start for governments, more is required and a focus on the purpose for the cyber security education is critical to identify different public policy requirements, career paths and education levels required.

4.6 Further Investigation with Informants

Two Universities (University of Melbourne and University College Dublin) and Hays Recruitment were invited to provide their views on the research and more broadly on the cyber security industry. Overall, their views reinforce the distinct gap between educators and industry and the requirements for both. University of Melbourne stated that ‘specialist cyber security courses undoubtedly have a role to play in the overall education framework. Whilst a gap in specialist skills is an issue, it is one that can be addressed both quickly and effectively through dedicated training, whether that be through mission-specific master’s programmes, like the one offered by UCD, or commercial training courses. Hays Recruitment on the other hand noted that ‘experience is the biggest requirement for employers and both industry certifications and academic qualifications do not rank as highly and are not considered nearly as relevant’.

The University of Melbourne stated that ‘specialist cyber security courses undoubtedly have a role to play in the overall education framework’. This aligns with comments from Hays Recruitment whereby ‘technical cyber security roles are specialised and require specific skillsets for each individual work roles. Generalist programs while providing an overview into
multiple areas don’t address the requirements for specialised work roles’. Hays Recruitment went further saying that they ‘actively work with industry in developing recruitment requirements for cyber security roles as the field is still immature’.

All informants agreed that work placements can be extremely valuable, in both the student’s education and their subsequent employability. As experience is seen by industry as the most valuable recruitment trait, there is a requirement for universities to consider this further. Hays Recruitment supported the viewpoint of students/employees starting in low level positions and moving into the relevant roles as their experience grew. UCD ‘works very hard officially through partnerships and through indirect industry contacts to assist students in finding work, either during (internships) or after finishing their courses’. This type of interaction assists in establishing the value of these programs to potential employers or recruitment agencies.

It is interesting to note that the University of Melbourne stipulate ‘that the evolution of cyber security threats out paces that of the corresponding training. It is important that we instil in our graduates the skills necessary to be able to independently undertake the constant education needed to perform well in the field’. All informants agreed that practical simulations and cyber ranges play an important part in developing the necessary leadership skills to evaluate and respond to an emerging threat. These skillsets are required to ensure there is a level of work based experience. UCD stay relevant through working closely with industry and subject matter experts. This provides courses that are specific, in depth and work role relevant ensuring the course materials are up to date. This also ensures that students who have participated in the course are recognised by employers and understand the KSA’s they would have acquired in undertaking the course.

There are currently high expectations on employees to have five plus years’ experience and have KSA’s in multiple areas. There could be a base for utilising lower skilled employees and training them in certain areas to fill a role due to the cyber security skills crisis. The requirement for practical skills and work integrated learning in courses and further industry-university collaboration is required to ensure programs are aligned with work role requirements and relevant. It benefits neither industry or universities if students undertaking these types of courses cannot find employment.

Other aspects affecting the employers is that not all roles require specific cyber security qualifications. There are courses that prepare technical students to undertake required work roles and have appropriate KSA’s. An example of this is software engineering, this is not specifically cyber security based but builds on large amounts of cyber security KSA’s. This is an area that requires further investigation into the benefit of establishing them as either specific cyber security named courses or re-enforcing the multi-faceted and multidisciplinary nature of cyber security. The final point of interest was that Hays Recruitment stated that they did not have major difficulty in filling the cyber security roles for employers in Canberra. This goes against the current trend of a skills crisis, if the roles are actively being filled. Though it should be noted that as the nation’s capital, Canberra has large amounts of workers from interstate and internationally come to specifically work for the Australian Public Service or industries that contract into government.

5. Discussion

Universities are places of higher learning that can both lag behind industry or be at the forefront of advancement and innovation, and many scholars simply choose to have nothing to do with
industry since they are pursuing less applied subjects. Universities must continue the vision of excellence in research and higher education, while pursuing beneficial partnerships with industry. Moreover, as this field of cyber security is still in its infancy, there could be case that many decision-makers in Australian industry currently do not know what they need in terms of employee training and education in this domain.

The initial survey of the student cohort, the results from both the comparison of work role KSA’s and the mission specific course examples demonstrate there is a gap in student expectations in undertaking the Master of Cyber Security and the future possibilities for employment. While students who already have a role in a cyber security position found they should be able to utilise their acquired KSA’s, the students who are not, may find it difficult to find future employment. These assumptions only look at the overall picture and not the other skillsets the students have relevant to potential employment. The comparison in work role KSA’s and outputs of the generalist master’s programs reinforce the message that industry reported in the ISACA and AISA surveys, whereby academic qualifications weren’t regarded highly. Moreover, it should be noted that Master's degrees can be vocational, but they can also be preparatory for further studies and research, such as a PhD, and can focus on the technical aspect of cyber security, as much as on applied activities.

It would be beneficial for universities, as the research asserts, to partner further with industry to establish career pathways for students, practical and work integrated learning opportunities and to ensure the programs are meeting key skills crisis work roles. Universities could investigate industry partnerships in ensuring career paths for students while studying and after graduation.

This last point is especially important for the universities who were awarded the ACSSE, as one of the key goals is to increase the number of highly skilled post-graduates with the job ready skills needed to work in Australian business and government to tackle emerging cyber security challenges.

5.1 Key Research Outcomes

The key research outcomes should be looked at by universities and industry to promote effective alignment between the educational outcomes and industry requirements.

- The Cyberspace Education Framework provides a valuable tool for analysis of education and training programs.
- The industry survey results demonstrate a gap between university offerings and industry’s requirements from them as education institutions. Universities have the potential to expand and amend their programs to meet industry needs.
- A move away from the “all in one” generalists curricula and instead offering distinct multi-faceted and multidisciplinary course streams would enable courses to be individually tailored to meet specific mission-specific requirements.
- Aligning program streams to industry vacancies could add value to Master of Cyber Security programs.
- Practical skillset application and development is vital for technical based programs.
- Workplace integrated learning is essential (if implemented correctly) and can provide valuable experience to students who are not in the industry or want to actively expand new skillsets (an example is outlined in section 5.2).
• Universities working with industry to provide internships/work placements could be a valuable promotion tool for universities.

5.2 Applying this Research

Adapting current cyber security education towards a necessary workplace-integrated learning program involves applying the methods and findings outlined above to mission-specific and role specific programs. The discussion below around possible planning for a new mid-career or early career Master’s degree illustrates what that might look like if UNSW Canberra were to undertake to prepare team leaders in advanced cyber operations for military and national security purposes. The proposal would involve consultation with the sectors and industries the courses are intended to support, principally but not exclusively Defence (the Australian Defence Force and Department of Defence), other national security agencies, and the private sector. Additional development of new courses may depend on additional funding, if only for the Government to incentivise fully integrated learning programs. Here is how a new process might unfold.

Mapping of the key KSA and attitudes for such a degree might ascertain, based in part on this paper, that the main gaps in current programs UNSW Canberra programs were:

(1) Knowledge: understanding of legal aspects of cybersecurity, as applied to rules-of-engagement for attributing sources of cyber-threat, mechanisms for referral to authorities of suspected criminality encountered in intelligence work, and techniques of offensive deterrence (active defence).

(2) Skills and abilities: mentored investigative or research skills in applying the techniques used on both unclassified and real cyber-ranges in medium complexity red v. blue exercises.

(3) Attitudes: practicums to develop successful attitudes to deal with the uncertainty prevalent in cyber attribution, the pervasiveness of cyber-operations, invasiveness of malicious intent and probing, and the deleterious effects of the mostly indecisive outcomes (i.e. no win/lose or reward).

UNSW Canberra with representation from Defence and Government could negotiate with cybersecurity industries with the necessary experience and security clearances to help develop and oversee three different integrated workplace learning programs: one for Defence, one for Government departments (State/Territory or Federal) and one for industries that provide essential national services such as finance, transportation and utilities. Private sector companies could agree to partner in developing the practicums: e.g. US Company A and UK Company B.

Stakeholders could work toward developing a formal degree program that would extend current cybersecurity master’s programs for one year (full-time equivalent) by including specialised integrated workplace learning programs into a second year, each of which leverages common existing subjects into more specialised purpose specific outcomes (defence, other government, industry—all of which have roles in cyber military operations). To raise the standard of education with high level academic input, a new funding model could include two industry chairs (US Industry A and UK Industry B) and two academic chairs (applied cybersecurity law

---

3 The author is grateful to Dr Keith Joiner, CSC, for his assistance in compiling an example to envisage how the research findings might be applied and with what consequences.
& cyber-range research operations). The academic subjects for the intensive knowledge component and practicum might be:

- **Semester 1 (Year 1):**
  - Cyber law (Applied legal Chair/Industry Chair B)
  - Cyber acquisition governance (Current Academic/Industry Chair A)
  - Advanced cyber security test and evaluation techniques (Current Academic/Industry Chair A)
  - Cyber Network Architectures (Current Academic/Industry Chair B)
- **Semester 2 (Year 1):**
  - Cyber Network Protections and Attributional Tools (Current Academic/Industry Chair B)
  - Cyber defensive techniques, including cooperative vulnerability testing (Cyber-range Operations Chair/Industry Chair A)
  - Cyber offensive techniques, including penetration testing (Cyber-range Operations Chair/Industry Chair A)
  - Cyber warfare strategic dimensions (international factors, hybrid warfare, hacker profiles, cybercrime etc) (Applied Legal Chair/Industry Chair B)
- **Practicum Year (Year 2):**
  - Research project (All)

The new programs could commence with new external funding for 25 students in each program per year (75 total), growing by a further 25 positions in each program each year over three years to a total of 225 per year. As the funding is provided by the government, only Australian citizens with a minimum security clearance would be allowed, while Defence students are subjected to additional clearances before the practicum phase. The delivery of classified Australian-only education programs in a university setting would be problematic and would be seen by many as contrary to the ethos of Australian universities. A cyber security institute and the Australian Government Department of Education and Training could partner to accredit the new integrated workplace learning program with reviews every two years. The first graduates are presented with both a Master of Cyber Security and a cyber security institute accreditation as high-level practitioners. The program becomes both an important feeder of graduates with recognised KSA in cybersecurity that are sufficiently experienced more quickly than current industry norms (i.e. 2.5 years c.f. 5 years), but could spawn replication in other cyber security education programs within Australia and abroad.

### 5.3 Areas for Future Research

There are five key areas for future research which should be undertaken to further investigate the educational outcomes and industry requirements.

- What the Australian cyber security industry wants and requires from education institutions.
- Educational outcomes and industry work roles is required to accurately map the broad requirements of the skills and education crisis.
- There is a key lack of relevant data on baselines and benchmarks on the effectiveness of cyber security education programs. More is required into investigating the relevance of all current programs focusing on cyber security and the true requirements of industry.
• Should there be a more hybrid model for cyber security education (a cyber security college) incorporating aspects of higher education, vocational education and training (VET) and industry certifications.
• Further research into establishing trainee or cadetship programs or similar would be beneficial for students to gain the necessary experience.

This research demonstrates that investigation into university courses and their alignment to work role KSA’s provides a valuable picture for both universities, industry and policy makers alike. Further investigation is required to ensure that all aspects, including KSA outcomes, skills acquired from practical projects, workplace integrated learning and the course learning outcomes are addressed more fully. This focus could ultimately shape public policy on key cyber security issues. A nation which is cyber resilient is essential for it to truly prosper in the digital information age.

6. Conclusion

The purpose of this research was to set out to investigate if the current Master of Cyber Security programs were preparing students for the workforce. The results note that more needs to be done in this space, but disruption is often hard to implement in large organisations such as universities. The results show that while student experiences are positive, alignment of courses offered with work role KSA’s is low. Overall, a course that moves more towards being mission-specific, purpose-driven and closely aligned with the work role KSA’s, would greatly improve the success of students moving into the workforce and the effectiveness of the courses offered. Universities need to promote their programs more broadly with industry to break the current viewpoints and perceptions. It is fair to say that in general, the relationship between industry and universities needs to be improved particularly with respect to the development of industry-integrated curricula, as has been argued for a decade (Koppi et al., 2008).

The requirement for purpose-driven and mission-specific cyber security education is increasing and will continue to become more relevant. This focus enables stakeholders to establish key educational programs and polices relevant to the particular requirement. The Cyberspace Education Framework provides a model to view cyber security education holistically within the public policy context. This method aims to ensure relevant pedagogical aspects are covered and identified. This enables baselines and benchmarks to be utilised. The paper tested the model against higher education examples and demonstrated that the model can be used for future reviews encompassing the alignment with work role KSA’s. This can then be utilised to create a cyberspace education maturity index that can be reviewed each year. Ongoing evaluation is critical to identifying strengths and weaknesses in existing programs and specific areas that need to be addressed.

In response to the initial question stipulated in this paper (are current Master of Cyber Security programs preparing students for the workforce?), this paper demonstrates a requirement for the realignment of courses to enable relevant work role KSA’s to be acquired by students during their studies. The government’s strong focus on cyber resilience must be understood. Australia has the opportunity to be a leader in cyber security education globally. This potential needs to be viewed with disruption in mind, with universities being open to new ways of operating in partnerships with industry. The requirement for universities to produce highly skilled post-graduates with the job ready skills needed should be viewed as an opportunity and the way forward.
References


cooper.pdf?ip=149.171.67.148&id=1709457&acc=ACTIVE%20SERVICE&key=65D80644F295BC0D%2EB811333C2AA88C82%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=870600112&CFTOKEN=261232928_acm_1482056585_11a76a18c179ee4aa8d75e5128b45db5 [Accessed 18 Dec. 2016].


