Teach A Man To

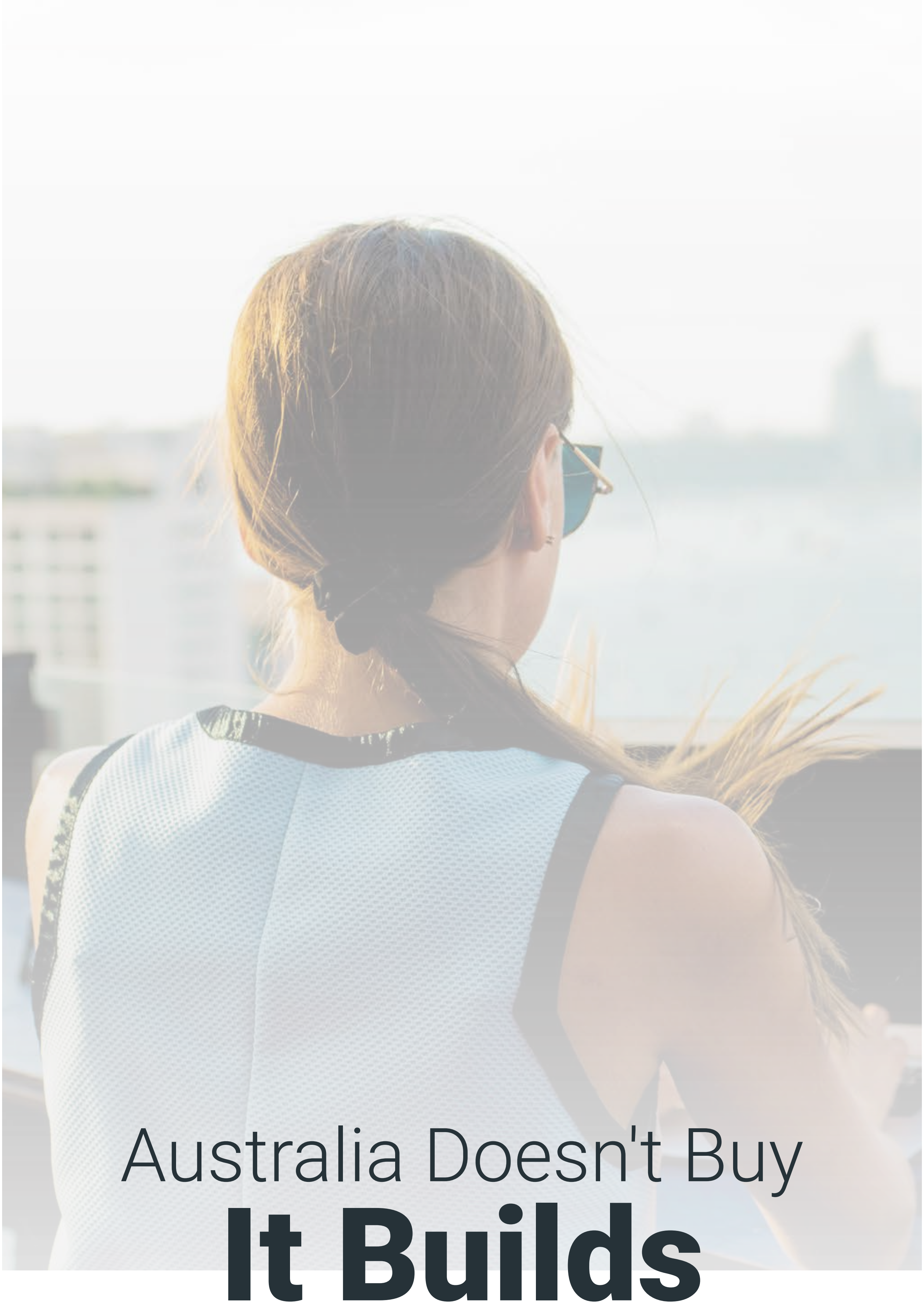
F.I.S.H.

<Future In Digital Security Human Resources/>

Future | In Digital | Security | Human Resources

Petition For Course Accreditation

Contents



Australia Doesn't Buy
It Builds

Industry Demand

Australia’s Industry Demand

The Teach A Man To F.I.S.H. Initiative

CONTRIBUTORS

Authored By:

Jesse Miller

Head Of International Development
& Government Relations

HackerU Global Education

Jessem@hackeru.com
+972.50.222.4978

Israel Trade Commission
Sydney, Australia

Forward

The Israel Trade Commission in Sydney operates under the Foreign Trade Administration, Israeli Ministry of Economy and Industry.

Our office goal is to promote, enhance and facilitate trade, investment and industrial R&D cooperation between Australia and Israel. Through a focus on the strengths and requirements of both the Australian and Israeli markets, the Trade Commission works to develop strategic bilateral partnerships through identifying exciting new investment opportunities and perform scouting activities for Australian companies and corporates in order to integrate excellent Israeli technology innovation.

The Israel Trade Commission is happy to support HackerU becoming a Registered Training Organisation in Australia to teach Australians how to build capacity for the purpose of protection against cybersecurity threats, a skill that is in shortage in an increasingly complex threat targeting Australia.

Israel is a global centre and a hub for tech innovation. A friendly and trusted country with enormous experience in Cyber tutoring and education. Israel has top scores on global indexes of economic competitiveness, a striking concentration of innovative people, a culture that promotes experimentation and daring, and governmental eagerness to create supportive conditions. Apart from Silicon Valley, Israel has the highest concentration of high-tech companies in the world.

Cyber penetration and protection skills are definitely growing in demand for the present and most certainly for the future. According to Reuters: Global demand for offensive cyber systems is expected to rise 39% by 2027 to $9.7 billion, according to defence research group Market Forecast, which identified companies in the United States, Israel and the European Union as dominating the market.

If Australia wants to become an economic powerhouse in the digital economy, they should adopt strategies that mitigate their geographically distanced workforce. HackerU’s education is a good initiative and one this office supports.

- Shai Zarivatch
Trade Commissioner
Israel Trade and Economic Commission
Embassy of Israel
AUSTRALIA

Executive Summary

The Australian Government released its National Cyber Security Strategy in 2016 and backed it with $230 Million Dollars. The report clearly identifies the problems, milestones, and goals to achieve.

This money was used to fund new initiatives to better the cyber security landscape in Australia and did not include standard government subsidies for students learning a trade, including studying cyber security.

The aim of the 2016 plan underpinned the urgency of which cyber security plays in every aspect of the Australian economy. However, some of the initiatives and programs created from government funding, according to recent reports, have not necessarily improved the cybersecurity landscape in a meaningful way, as this report will aim to prove.

Teach A Man To F.I.S.H. is a trade initiative. It is precisely in line with the Australian Government's goals in improving the cyber security sector. The initiative focuses on education, innovation and trade with Israel, arguably the world leader in cybersecurity. Israel is the country with the second-largest cyber security market share internationally, despite its size, limited resources, and small population

The initiative aims to fill the existing cyber security skills gap, allowing Australia to develop its own domestic cyber security industry, and make it an internationally competitive powerhouse.

This initiative would create thousands of high paying jobs in Australia that are difficult to automate and would provide financial stability and security for graduates.

Israel's largest and most respected cyber security training organization is uniquely positioned to take someone with no experience in computer science, IT, or software development. They select potential students based on aptitude alone, and efficiently produce a skilled, professionally certified, and work-ready cyber security professional in minimal time.

> *" This initiative would create thousands of high paying jobs in Australia, that are difficult to automate and provide financial stability and security for graduates.*

As cybercrime costs Australians an estimated 1 billion dollars per year, and as cybercrime and cyber-espionage become increasingly sophisticated, it's imperative that Australia find solutions. This will enable them to maintain their reputation as a safe and secure environment for business, and continue the uninterrupted economic growth they have experienced for the past decade.

This is echoed in the AustCyber report titled "Australia's Cyber Security Sector Competitiveness Plan 2019 update" stating:

> *"Cybersecurity is not only a dynamic sector offering a new source of economic growth and prosperity to Australia, it is also an enabler of growth through digital transformation in every sector to the economy. As businesses rely on the confidentiality and integrity of digital information, a strong domestic cybersecurity sector is critical for Australia's competitiveness and international reputation as a trusted place to do business, and for the nation's continued economic growth."*

AustCyber identified the key issue preventing growth as a skills shortage, and leads with it in its key findings. They call on the government to act urgently:

"To seize the extensive opportunity Australia needs to act urgently.

Several hurdles are making it difficult for Australia to fully harness existing advantages and develop a sizeable world-class cyber security sector. To capitalize on the enormous opportunity in cyber, Australia must address its skills shortage."

"To seize the extensive opportunity Australia needs to act urgently.

Several hurdles are making it difficult for Australia to fully harness existing advantages and develop a sizeable world-class cyber security sector. To capitalize on the enormous opportunity in cyber, Australia must address its skills shortage."

- AustCyber Australia's Cybersecurity Competativeness Plan

Citation

This initiative uses government reports which identify the issues that are stunting Australia's cybersecurity growth. Primarily a workable solution for producing market-ready manpower through the education system.

This initiative doesn't aim to overtly criticize Australia's efforts. It seeks to analyze the effectiveness of its current initiatives, and offer alternative methods to solve stated problems by using industry leaders' methods of solving the same problems as an example.

Only official documents were used in the following initiative, and are frequently quoted.

Primary Documents Include:

◊ **Australia's Tech Future - Delivering a strong, safe and inclusive digital economy**
◊ This report was produced by the Ministry of Industry, Science and Technology
◊ The full report can be found here: https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf

◊ **Australia's Cyber Security Sector Competitiveness Plan - 2019 Update**
◊ This report was produced by AustCyber or the Australian Cyber Security Growth Network - This group was created as part of the 2016 initiative.
◊ The full report can be found here: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019

◊ **2017 Employer Satisfaction Survey (ESS) - National Report**
◊ The report was produced by QILT or Quality Indicators for Learning and Teaching
◊ The full report can be found here: https://www.qilt.edu.au/docs/default-source/ess/ess-2017/2017_ess_national_report.pdf?sfvrsn=19b2e33c_12

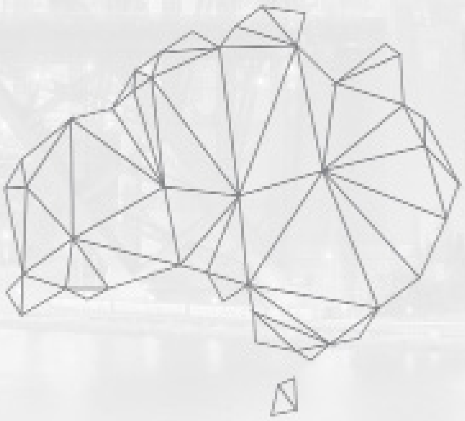
◊ **2019 Employer Satisfaction Survey (ESS) - National Report January 2020**
◊ The report was produced by QILT or Quality Indicators for Learning and Teaching
◊ The full report can be found here: https://www.qilt.edu.au/docs/default-source/default-document-library/ess-national-report-2019.pdf

Supporting research Documents (But Not Quoted) Include:

- Academic Centres of Cyber Security Excellence Program Guidelines
- ACSC - Australian Cyber Security Centre 2017 Threat Report
- The Commonwealth Cyber Security Posture In 2019
- 22334VIC Certificate IV In Cyber Security (Guidelines Victoria DET)
- Education and Training Reform Act 2006
- Users Guide To The Standards For Registered Training Organisations 2015
- Australian Qualifications Framework 2nd edition
- Standards For Registered Training Organizations 2015
- Standards For VET Accredited Courses 2012
- National Vocational Education And Training Act 2011

The goal of this initiative is to offer an alternative that would have no cost to the Australian Tax Payer while allowing taxpayers to reap long term economic benefits. Potentially creating thousands of jobs, contributing to stopping the hemorrhaging of cash that is caused by cyber-attacks, add potentially billions of dollars to the Australian economy, and bolster Australia's national security.

F.I.S.H.



- Future
- In digital
- Security
- Human resources

Part 1

Current Status Of Australian Cybersecurity

The Necessity of Cybersecurity for Australia's Future

"Data from the Office of the Australian Information Commissioner (OAIC) indicates that 58 percent of Australians avoid dealing with a business if they have concerns about that business"

Cyber security is not an industry that works in an economic vacuum. It permeates all industries and areas of commerce: from tourism to agriculture; from e-commerce to banking. It reaches so deep into the economy of any country, that a lack of strong cyber security could damage a nation's reputation for international commerce or have serious national security implications.

Australia's Tech Future - Report

Cyber security has been identified by the Honorable Karen Andrews, Minister for Industry, Science, and Technology as being a driving force of all Australian future industries. In her report titled 'Australia's Tech Future', she stated;

"*In order to continue our run of over 27 years of uninterrupted economic growth, Australia must seize the significant economic and social opportunities that digital technologies bring*"

-Hon. Karen Andrews (Australia's Tech Future)

The 52-page report that follows marks out Cyber security as a major driving force in the future of Australia's economy, and is essential for the growth of all industries, not just the cyber security industry or the tech sector.

"*A greater focus on cybersecurity by Australian businesses will see significant benefits to the wider economy, and could lift business investment by 5.5 percent by 2030, creating 60,000 new jobs*"

The report also admitted that cybercrime is currently estimated to cost Australians more than 1 billion dollars

The report calls on all areas of Australia to understand the urgency in addressing this matter. What remains key to future positive outcomes is to also address the driving factors that need to come together to make Australia's cyberspace a safer place.

"To take advantage of these opportunities and reduce Australia's exposure to cyber threats, the Government, industry, and the education sector need to work together to inform the workforce and address the significant shortage of cyber skilled experts"

When speaking about general digital literacy in the Australian public, the report states:

"*Individuals, businesses, and governments need to work together to support a workforce with the skills in demand so we can have a modern, competitive economy.*
All Australians have a role to play:

- *Workers should identify opportunities to continue to update and develop new skills*
- *Businesses need to invest in their workforce*
- *The government will support people to evolve with their jobs and transition into new ones.*"

It identifies that there's a shortage of skilled workers in the cyber security profession. And comments that:

"*Businesses, employees and entrepreneurs are keenly aware that not having the right digital capability in their workforce will hinder business innovation and growth, putting Australian businesses at a competitive disadvantage in the global economy*"

The report identifies education as a spot for improvement. Increased flexibility and innovation are clearly needed.

"To help workers to transition or re-skill, the education sector needs to embrace non-traditional forms of study. This could include micro-credentials, which recognize informal and formal learning in specific areas and offer an efficient way to ensure that employees are keeping their skills relevant and certified."

"A greater focus on cybersecurity by Australian businesses will see significant benefits to the wider economy, and could lift business investment by 5.5 percent by 2030, creating 60,000 new jobs"

-Australias Tech Future

It calls on the government to address these needs:
"Governments and industry need to provide support for workers needing to up-skill, re-skill or transition into new areas of employment, whether this be early in their career or when the person is closer to retirement"

> *“The government will work with academia to capture the expertise that the sector can bring to a range of digital economy issues”*

The urgency is supported by The Australian Cyber Security Centre Threat Report 2017 reveals that there is an increase in frequency, scale sophistication, and severity of malicious cyber activity against Australia’s national and economic interests.

AustCyber - Australian Cyber Security Sector Competitiveness Plan (2019 Update)

Despite having a developed and robust economy, Australia’s tech and cybersecurity sectors are lacking relative to other countries with a similar status as economic leaders. This all stems from an acute skilled worker shortage.

AustCyber introduces their report with a call to action:

> ***“More needs to be done to ramp up the momentum over the next 12 months - Including targeted government and industry investment and infrastructure to support commercialization and innovation, and the establishment of a national platform for measurable and scalable cyber security skills development and workforce growth”***

They justify the strong language used in the call to action by explaining that cyber security is essential not just for the cyber security industry, but for every industry where Australia finds its current strengths:

“A globally competitive Australian cyber security sector will ultimately underpin the future success for every industry in the national economy. A consolidated effort is needed to continue to build early success and sustain Australia’s competitiveness and strategic advantages in the creation and commercialization of cyber security products and services”

When addressing the challenges, AustCyber’s report leads with the skilled worker shortage in their key findings. They reveal the following:

“New research, undertaken exclusively for this (2019) updated Sector Competitiveness Plan, draws on a range of job market data, showing the skills shortage in Australia’s cyber security sector is more severe than initially estimated and is already producing real economic costs.

Australia may need almost 17,000 additional cyber security workers by 2026 for the sector to harness its full growth potential. The workforce shortfall has significant economic consequences. In 2017, the domestic cyber security sector is estimated to have *forfeited up to $405 million in revenue, which companies could have generated if they had been able to find enough cyber security workers to fill existing vacancies."*

The required 17,000 additional cyber security workforce assumes that these workers will be highly skilled, and meet employers' satisfaction. **There's also an estimated 60,000 that will be required if Australia rises to the occasion and works at full capacity to produce not only a large number of workers but highly skilled workers**

Although AustCyber compliments universities for taking action, there are three questions that arise.

1. Is it enough?
2. Is it efficient?
3. Is it currently working?

> ***"Australia may need almost 17,000 additional cyber security workers by 2026 for the sector to harness its full growth potential. The workforce shortfall has significant economic consequences. In 2017, the domestic cyber security sector is estimated to have forfeited up to $405 million in revenue, which companies could have generated if they had been able to find enough cyber security workers to fill existing vacancies."***
>
> -Australia's Cyber Security Competiveness Plan 2019 Update

Will Training Institutions Produce Enough Workers?

To address the first question the report states:

"*Approximately half of all universities in Australia are now offering cybersecurity as a specific degree or a major in IT or computer science degrees.*"

It also gives mention to VET certificate and degree level courses. All things considered, the report has the following to say about the increase in the workforce:

"*It is expected that the number of graduates could quadruple from around 500 per year in 2017 to 2000 a year in 2026, based on the current course offerings by cyber security education providers.*"

Is that enough? Absolutely not. With the report's stated estimate of the number of graduates needed to be around 17,000 skilled workers.

In mid-2020, the education system is currently not reaching those numbers and we can realistically expect them to reach that capacity in the later years of the plan. Even in the

most optimistic estimates whereas the education system was currently reaching that capacity, that would leave thousands of required, essential roles unfulfilled. **The report confirms this:**

> *"However, this still leaves a significant shortfall of workers in the medium-term. Analysis for this Sector Competitiveness Plan shows there are risks to mobilization in the education system, and more action is required,"*

The report calls for action in the following way:

"Australia needs to nurture early interest in cyber security to attract the best and brightest to the sector, continue to ramp up cyber security education and training, create industry-led professional pathways. We also need to help workers with related skills transition from the wider IT sector and other industries into the diverse range of cyber security technical and non-technical roles required by employers"

Is Training Efficient?

The Skills Gap is reaching into research and development. As the skills gap begins with a lack of public interest in cyber security as a field of study. The report labels that as the 2nd key finding, stating:

> ***"Australia continues to demonstrate excellent and world-leading cyber security research capability. However, there are signs that its system of research and commercialization is less efficient in other leading cyber security nations such as the US and Israel"***

While both the US and Israel have a skills gap like the rest of the world, they have different strategies to deal with them.

The U.S. mainly seeks the best and the brightest from an international pool of talent, and uses its capital might to staff what is required. They also use one country with the least deficit of skilled workers per capita for more cost-efficient labor. This country is Israel.

Israel deals with the worker deficit with innovative solutions in their education system.

Looser regulations for government-approved schools allow flexibility in education materials and marketing. The Education system in Israel produces well over ten thousand cyber security graduates per year. This initiative advocates for such a system as it is the core reason for the significant Israeli success in cyber security, and its success in creating thousands of jobs from the US and other international companies because of its labor advantage.

Is The Education's Quality Meeting Comercial Demands?

AustCyber makes mention in its report that there is a lack of accurate measurement. However, it also states that the majority of cyber security professionals are coming from an IT background. The closest we can get to empirical data on the commercial viability of graduates are from the Employee Satisfaction Survey. The ESS measures by broad category, IT which also encompasses cyber security.

Data From ESS Reports 2017 - 2019

To understand the effects the current initiatives are having on the cyber-skilled workforce, we've drawn information from two official ESS reports.

The Employer Satisfaction Survey report is meant to be a Key Performance Indicator for the education system, and to judge fairly if education in various sectors is keeping up with commercial demand.

Since the $230 million dollars was earmarked by the government and spent through various initiatives, accurate measurement is essential to understand the initiative's impact.

ESS 2017

According to the 2017 National Report of the ESS (*Employer Satisfaction Survey*) sponsored by QILT (*Quality Indicators for Learning and Teaching*) showed the following:

Employer satisfaction with graduates attributes and overall satisfaction indicated that 93.3% of Employers found that they were satisfied with graduate technical skills - nonspecific to IT.

Specifically, according to the 2017 Employer satisfaction by broad field of education showed the following for Information Technology:

Catagory Satisfaction	%
Foundation Skills:	95.1%
Adaptive Skills:	91.1%
Collaborative Skills:	90.4%
Technical Skills:	95.5%
Employability Skills:	85.7%
Overall Satisfaction of IT graduates:	82.1%

According to the 2017 National Report of the ESS (*Employer Satisfaction Survey*) sponsored by QILT (*Quality Indicators for Learning and Teaching*) showed the following:

Employer satisfaction with graduates attributes and overall satisfaction indicated that 93.3% of Employers found that they were satisfied with graduate technical skills - nonspecific to IT.

Specifically, according to the 2017 Employer satisfaction by broad field of education showed the following for Information Technology:

ESS 2019

According to the most recent Employer Satisfaction Survey (2019), there are either unremarkable changes or negative outcomes.

92.7% was the rating given to employer satisfaction with graduate attributes and overall satisfaction down from 93.3%; a reduction of 0.5%

Employer Satisfaction by the broad field of Information Technology which includes Cyber security rated satisfaction in a number of categories as follows:

In every measurement in Employer satisfaction of graduates of the IT field, there is a marked decrease in satisfaction; most importantly in technical skills, and most notably in overall satisfaction.

Employer satisfaction with graduates from IT-related fields relative to other fields of study has not changed, while the lowest percentage is now 75% belonging to Creative Arts, IT still hovers among the lowest in satisfaction.

Catagory Satisfaction	%
Foundation Skills:	91.5%
Adaptive Skills:	86.9%
Collaborative Skills:	87.9%
Technical Skills:	92.3%
Employability Skills:	82.1%
Overall Satisfaction of IT graduates:	80.6%

In Another Survey, Measuring The Importance Of Qualification For Current Employment By Broad Field, Graduates, and Supervisors in the Information Technology field rated the qualification as ‘Very Important’ or ‘Important’.

Rated IT Skills ‘Important’ or ‘Vary Important’	%
Graduates	**41.1%**
Supervisors	**48.4%**

To put it in perspective, the highest rating by Graduates and Supervisors is for “Health”; earning a rating of 70.2%, and 79.2% respectively. The percentage of both graduates and supervisors believing IT is ‘very important’ or ‘important’ since 2017 has increased by 1.1% 6.2% respectively.

There are two thought-provoking takeaways from this slight increase.

1. That both graduates and supervisors are realizing that IT-related skills are increasingly important for the future.

2. The fact that the ratings in 2017 were relatively low, and the fact that they haven’t increased significantly from 2017 to 2019, says something about the state of the Australian economy. The fact that the numbers don’t come close to that of “health” as a broad field of study shows that the Australian economy isn’t advancing in the digital age at a speed comparable to their commonwealth counterparts. If Australia’s industry was increasing its presence in the digital economy, the importance of this skill would be universally acknowledged to be either ‘important’ or ‘very important’ regardless of industry. This fact is further referenced in other reports and initiatives produced by or presented to the Australian government.

The most important survey study collected information about the "Extent to which qualification prepared graduates well or very well for current employment, by broad field of education, 2019" The respondents answered the following for the Information Technology field.

IT Qualification Prepared Graduate 'Well' or 'Very Well'	%	+/-
Graduates	**84.4%**	+0.01
Supervisors	**90.4%**	**- 3.00**

This number has not significantly increased for graduates, but for supervisors, the number is significantly down from the 2017 report.

Supervisors gave a rating of 93% in 2017, a decrease for Supervisors' satisfaction with graduate's readiness for their trade of 3%, and 84.5 for Graduates. The minimum increase of 0.1%

To give perspective the lowest satisfaction belongs to the Creative Arts category, at 76.2% - Graduates and 81.4% - Employers

ESS Data Interpretation & Conclusions

Perhaps these numbers are the most telling about the state of the Australian Education System in interaction with industry to modernize and advance in the digital space.

While overall ratings seem high, it's below the median score across all categories. Furthermore, there is a notable decrease from 2017 - 2019.

Education in the digital sphere is faster paced and more dynamic in nature than any other category. A decrease in this survey may very well indicate that Universities and RTOs are not keeping pace with commercial changes regarding practices and technologies.

By its very nature, a university degree may not be the most suitable option for workers in many of the research fields encompassing the broad category of Information Technology. Even if the degree program solely focused on technical skills over a 3 year time frame, what was learned in the first year may be irrelevant by the time the student earns his degree.

This is especially true for the essential field of cyber security, where practical application and ability to adapt to new technologies and threats is one of the only considerations. For employers to be satisfied with a cyber security professional he must have these skills and be completely up to date with current threat prevention techniques that develop at a rapid pace.

> ***"A decrease in this survey may very well indicate that Universities and RTOs are not keeping pace with commercial changes regarding practices and technologies."***

Problem Solving To Meet The Sector Competitiveness Plan's Goals

While currently over half of the universities in Australia offer some sort of qualification in cybe rsecurity, and the inclusion of cyber security certificate level and diploma level qualifications in TAFES and independent RTOs are a step in the right direction, the system has some impediments to achieving AustCybers proposed goals.

This Initiative identifies the following:

1. Creating a system that simulates working scenarios and focuses on training is extremely expensive to build and maintain.

2. There are only 4 government-approved VET courses. They do not cover all areas of cyber security and leave out critical specializations.

3. Many RTO's and TAFES are not solely focused on cyber security. Because of this lack of specialization and focus, a simple cost-benefit analysis may disincentivize existing RTOs from cyber security when there are far more profitable courses with less overhead and marketing capital requirements to generate profit.

4. There has been a priority set by the Australian government to produce more skilled workers. However, it seems the priority has not been adequately communicated to the regulating bodies of Education Institutions such as ASQA. For outside education specialists to receive the benefits of the Australian education system, a lengthy and expensive audit process awaits them. Setting up in Australia as an RTO, proposing courses to the government for accreditation, and becoming approved for critical subsidies for students is a difficult and lengthy process that can deter the creation of specialized training centers.

AustCyber Sector Competitiveness Plan 2019

AustCyber as of 2019 estimates that the global cyber security market is worth around US$145 Billion dollars. They estimate that it will grow to US$248 Billion by 2026.

It states:

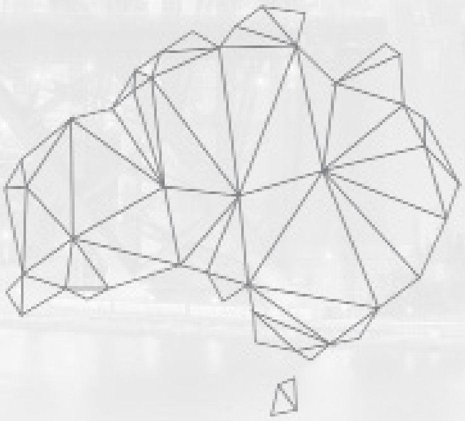
“Roughly three quarters of the global expenditure on cyber security comes from cyber security ‘users’ (organizations and Individuals seeking to defend themselves against malicious cyber activity) purchasing the products and services of external cyber security ‘providers’ (both specialist cyber security companies and IT or telecommunications companies with cyber security offerings). The remaining quarter of spending covers all internal expenditure on cyber security, mainly the cost of employing in-house teams with specialist cyber security skills.”

“Analysis based on available market data and expert interviews suggests this trend will accelerate in the future. While money spent on in-house or internal cyber security functions is expected to grow by around 7.2 percent each ear to 2026, global spending on external cyber security products and services is set to increase 8.4 percent annually over the same period.”

Further opportunities for Australia are found regionally if Australia can develop a healthy cyber security industry:

“Indo-Pacific countries have emerged as significant buyers of cyber security solutions, adding to the market opportunity for Australian providers”

F.I.S.H.



- Future
- In digital
- Security
- Human resources

Part 2

Economic Incentives

Current Australian Market And Economic Landscape

"Australian demand and employment is dominated by outsourced cyber security services" - "Software and hardware markets are dominated by direct imports"

The report makes key points as follows:

- ***"Total expenditure is A$5.0 billion in 2018***
- ***A3.8 billion spent on external cyber security 2018***
- ***A1 billion on internal cyber security functions***
- ***Strong cyber security will enhance Australia's global reputation as a trusted and secure place to do business***
- ***Foundation for future success of all industries in national economy"***

Australia is considered to be one of the greatest services hubs in the world.

Its education system is ranked among the top of the world.

As a country, it appears to be ripe to take advantage of the multi-billion dollar global cyber security market. The report admits the current situation is at odds with these well-known strengths of the Australian economic landscape:

> ***"Given the small scale of the domestic market, Australia will struggle to become globally competitive in all segments of the cybersecurity sector."***
>
> -Australia's Cyber Security Competiveness Plan 2019 Update

"Many Australian cyber security service companies are still failing to harness their full export potential. This is at odds with evidence that Australia is considered to be a services hub, with Australian business generally earning much more revenue (relative to national GDP) from services than their peers elsewhere in the world. Cyber security companies could do more to make use of this country-specific advantage"

The report gives the inevitable outcome if Australia doesn't make changes to advance this sector of the economy:

"Given the small scale of the domestic

market, Australia will struggle to become globally competitive in all segments of the cybersecurity sector."

AustCyber admits that there are limited resources available, and they propose shifting those resources to software and services.

Another problem outlined regarding internal demand for cyber security professionals is described in the following terms.

"Small and medium-sized enterprises make up around 95 per cent of all Australian businesses. These businesses may lack the scale and resources to run in-house cyber security management teams."

Domestic Market & Foreign Companies

"Currently there are no local companies among the 15 largest software providers by value in the Australian cyber security market. The combined market share of Australian companies is estimated to be less than five per cent"

Many international cyber security companies do have a presence in Australia and do serve the Australian economy by creating jobs. However, many of those jobs are service or sales related.

With a larger skilled cyber security professional talent pool, Australia could capture the benefit from more international presence hiring for technical roles. Workers could use their experience gleaned from these conglomerates to create a competitive marketplace for domestic Australian start-ups.

The report confirmed that foreign companies dominate the domestic job market:

"Foreign service providers with local operation remain the largest employer in Australia's external cyber security market"

With multinational corporations employing around 7,000 cyber security professionals.

"They are only exceeded by internal employment of cyber security teams, which is estimated to be around 9,000 workers"

Segments

The report divides market opportunities into three segments:

1. Hardware

2. Software

3. Services

Hardware

While this is not identified in the report as the strongest point in Australia's future, there is no reason why Australia should not focus on this essential part of the market. IT equipment is estimated to increase by 6.9 Billion US by 2026 with a growth rate of 6.5% per year.

The Wassenaar Arrangement can limit exports of some cyber security products for use in defense. However, currently, Australia isn't the leader in its own domestic market.

The report states:

"Hardware production supports an average of 4.6 full-time jobs per US $1 million of annual revenue generated, a labor intensity that ranks between software and service"

Software

"Software represents the cyber security sector's second-biggest product type"

As opposed to hardware, AustCyber identifies software as a massive potential segment in which Australia can realistically achieve a competitive stance in the world. The benefits for Australia to grab part of the global market share are explained:

"In the seven years to 2026, external demand for cyber security software is expected to increase at an average annual rate of 9.5 per cent."

Also as opposed to hardware, which is subject to regulation for national security concerns, software is highly exportable.

"Companies domiciled in the US control 61 percent of the global market, while Israeli companies dominate around 18 per cent."

This segment benefits the Australian economy in massive job creation. Not just for domestic companies to become an international player in the world market, but for foreign companies to set up bases of operation. Tens of thousands of jobs can possibly be created if Australia can increase its human capital.

Software supports *"an average of 4.0 full-time jobs per US$1 million of annual revenue. Cyber security jobs are typically of very high quality and hard to automate, requiring high-skilled and well paid staff."*

Services

AustCyber marks cyber security services as an immediately attainable growth sector. The advantages of creating a robust domestic market can have a tremendous impact on the Australian economy as a whole.

"Companies in the security operations segment attract almost 45 per cent, or US$29 Billion, of the entire global spending on external cyber security services."

The growth potential is noted:

"From 2018 to 2026, the global spending on external cyber security services is expected to increase by 8.1 per cent per year. Growth is expected to be strongest for security operations, with an additional US$56 billion in demand forecast over the period to 2026"

The job potential is also the highest in this sub-sector

"on average, services support 6.4 full time jobs per US$1 million of annual revenue, marking the highest rate of job creation among the three product types"

Segments Summary

"In the hardware and software segments, where the current revenues (relative to national GDP) of Australian companies and foreign companies with core operations in Australia are significantly lower than the equivalent world average signaling a comparative disadvantage.

Even if Australia goes about 'business as usual' the sector could more than double from 2.2 billion in 2016 to 4.7 billion in 2026"

However AustCyber makes a point that the economic advantages are markedly different if Australia makes a concerted effort to solve some of the underlying problems plaguing the domestic cyber security industry. Chiefly among them, mentioned countless times in the report is the skills shortage.

> *"Revenues in the domestic cyber security sector could increase to A$6.0 billion in 2026, which equates to an annual growth rate of almost 11 per cent over the decade."*

AustCyber on The Consequences Of The Skills Shortage

"The workforce could grow even further if Australia can address the current skills shortage" --- "If Australia could match the performance of global leaders such as the US and Israel, the cyber workforce would expand to almost 60,000 with industry revenue of $11 billion in 2026"

AustCyber Identifies the following as key takeaways from their report on the underlying problems in the performance of this essential sector:

- *"Severe shortage of job-ready cyber security workers*
- *Nearly 17,000 more cyber security workers needed by 2026*
- *Education providers increasing cyber security courses, with number of graduates could quadruple to 2,000 a year by 2026*
- *But growth is not sufficient to meet medium-term shortfall."*

To accentuate the importance of cyber security workers, not just to the sector but to the economy as a whole AustCyber affirms that:

"Strong cyber security skills and capabilities are a key driver of economic activity across the Australian economy and are critical for Australia's future prosperity."

They describe the current status of the educations systems ability to deal with this shortage as follows:

"Current growth is insufficient to cover the rapidly increasing demand for cyber security specialists

Analysis undertaken for AustCyber's inaugural Sector Competitiveness Plan in 2017 indicated that Australia is facing a severe shortage in specialized cyber security workers

New analysis for this updated 2019 plan reveals that cyber security skills gap is larger than initially anticipated and is costing both the sector and the broader economy

New education programs are critical for filling the skills gap in the long-term"

While the workforce has grown at a rate of 13% over the past 3 years, the pace is at a crawl compared with both the national and international demand. Most notably, the workers who are transitioning to cyber security are doing so from a previous role in the IT industry. They are essentially taking away resources from another important sector to fill the gap.

"Workforce growth has been driven by workers transitioning from adjacent sectors such as IT."

> ***"New education programs are critical for filling the skills gap in the long-term"***
>
> -Australia's Cyber Security Competiveness Plan 2019 Update

Shortage Statistics

The most recent numbers in four measurements point to a critical situation:

Wage Premium	$
Cyber Security Average	**$ 112,000**
IT Average	**$ 100,000**
Professional Services Average	**$ 94,000**

Recruitment Failure Rate	% Of Vacancies Left Unfulfilled
Cyber Security Average	**42 %**
IT Average	**33%**
Best Performing IT Catagory (System Admin)	**22%**

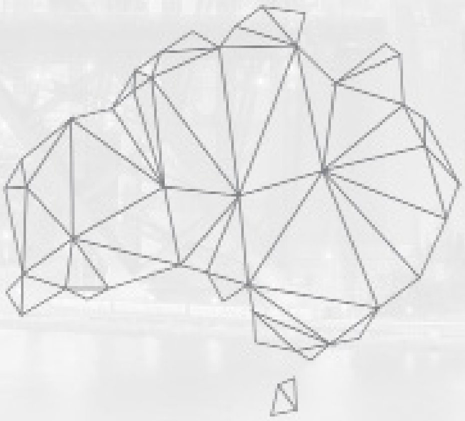
Recruitment Time	**20 % - 30 % Longer Than Average**

> ***"The cyber security sector is estimated to have forfeited up to $405 million in revenue and wages in 2017, which it could have generated if companies had been able to find the cyber security workers to fill existing vacancies."***
>
> -Australia's Cyber Security Competiveness Plan 2019 Update

And finally, the report suggests that the skills shortage effect is far-reaching and goes beyond cyber security as a sector of the economy. It already reaches into other industries:

> *"anecdotal evidence suggests that the shortage of cyber skills is already causing organizations to slow their digital transformation"*

F.I.S.H.



- Future
- In digital
- Security
- Human resources

Part 3

This Initiative’s Role In Developing Australia’s Cybersecurity Economy

Introduction

> *"Israel, traditionally boasting some of the highest defense spending in the world, also provides strong government support for cyber security R&D. Israeli companies form the second-strongest vendor group in the global market for cyber security software, accounting for 18 percent of total sales worldwide. Israel's Office of the Chief Scientist is frequently cited as the country's largest single investor in cyber security research, but official budget numbers are not readily available"*
>
> - AustCyber Australia's Cyber Security Competitiveness Plan 2019 Update

The Teach a Man to F.I.S.H. initiative focuses on the importance that international trade can play in addressing all these issues.

We've named this initiative "Teach a Man to FISH" derived from the well-known proverb "If you give a man a fish, he eats for a day. If you teach a man to fish, he eats for a lifetime.

F.I.S.H. stands for:

- ***Future***
- ***In Digital***
- ***Security***
- ***Human Resuources***

The reason why the initiatives name was chosen was to describe an alternative to the status quo.

The status quo that showcases the scenario where international trade in cyber security is dominated by buying foreign companies' products and services. For Australia, this has only served to give the proverbial man a fish.

This initiative outlines a way to export the fundamental reason for Israel's excellence in Cyber security:
Human resources created by innovative, flexible, and up to date education systems and professional training programs.

The Initiative offers a hand up for Australia to develop its own cyber security ecosystem. The resulting momentum will ultimately provide the essential resources so Australia can build its own cyber-economy to become first in the Australian national market, and to compete globally.

This method of trade between Australia and Israel fits more accurately the second part of the proverb. To "teach a man to fish, so he eats for a lifetime"

In the rest of the world, including the United States, a cyber security professional generally makes an annual salary that is on par with a doctor or lawyer if not more.

The United States addresses this issue with its capital might.

Israel addresses this issue with an innovation-in-education approach, creating an unmatched workforce in cyber security.

The Israeli education system creates a constant downward pressure on the salaries of workers and a constant flow of manpower. These conditions enable cyber security startups to have the ability to consistently arise from the tiny desert nation. Major international players have started and continue to be domiciled there, and many of the United State's giants of the cyber security industry have large offices in Tel Aviv to take advantage of Israel's relative surplus of high-skilled manpower.

Israel is number two in the world for market share, but arguably number one in cyber security. It all starts with a skilled workforce. This initiative offers to deliver that workforce by exporting its method for creating it.

A unique, up to date, and flexible education system designed to meet the immediate needs of industry and achieve the student's qualification in the shortest period of time is needed. It's evidenced in the number of official reports mentioned in this initiative.

A Private Education Provider, HackerU has played a major role in Israel's Cyber Boom

◊ **HackerU is an educational institution specializing in cyber-security. It has been training students in Israel for over 20 years and currently is a major force in creating this unique environment supporting unprecedented economic growth in the Tech Sector.**

◊ **HackerU has developed unique, proprietary technology, which simulates real-world scenarios for defensive and offensive training. The development costs are in the millions, and it takes significant financial overhead to maintain.**

◊ **The price has paid off. HackerU's graduates, many of whom had no prior experience or education in the tech sector, graduate within 6 months and have an 88% job placement rate. A testament to HackerU's commercially accepted qualifications.**

◊ **HackerU is on contract with the Israeli government to up-skill and re-skill essential workers for national security.**

◊ **HackerU produces over 7000 graduates per year to the commercial sector**

◊ **HackerU has unparalleled marketing and sales experience to enroll students in their programs. Students that may have never considered a career in tech, let alone cyber security.**

◊ **HackerU accepts students based on aptitude, with no prior knowledge of the industry or even IT related fields required. This vastly expands the pool of potential future cyber security professionals.**

- ◊ The Ad budget HackerU plans to spend only on the first month of operating in Australia, will be reaching an estimated 200,000 Australians per month.
- ◊ The budget is expected to grow substantially each quarter
- ◊ This ad budget will not only drive awareness of its brand. HackerU's investment will also create a pro-social public relations campaign. It will raise awareness of the importance of cyber security as a career choice.
- ◊ HackerU has both offensive and defensive programs. HackerU prepares students for internationally recognized proficiency exams such as the CE-H and OSCP
- ◊ HackerU offers a job guarantee and assists with job placement after graduation, serving as a direct connection between manpower and industry.
- ◊ HackerU is the most widely recognized and respected name in cyber security training in Israel and works with major universities in the US, Europe, and Asia to deliver relevant, current, and thorough training for individuals, corporations, and governments.

HackerU and The Teach A Man To F.I.S.H. Initiative

HackerU has decided to enter into the Australian Education System as a Registered Training Organization, and to partner with Australia as a whole in the goal of advancing the Australian economy.

In this initiative, it set forth a pathway, with no expense to the Australian taxpayer, to allow Australia to grow its own cyber security sector; to create their own products and services so domestic Australian companies can become the market leader in Australia, and compete on the global stage.

Together with the Australian government's report: *Australia's Tech Future* and initiatives set forth within, and the latest AustCyber's report " *Australia's Cyber Security Sector Competitiveness plan*" - HackerU believes its methodology is precisely in line with the goals set by the government, The Minister of Industry, Technology, and Science, The Department of Education, and AustCyber.

It can change Australia's tech landscape for the better and can play an integral role in reaching the goals set by the Australian government and its supported organizations to make Australia a world leader in cyber security and in the broader tech industry.

The Goals of this Initiative include the following:

1. **Open a Dialogue between executives at HackerU, the Minister of Industry, Technology and Science, and the Minister of Education and Training** - about how we can work together to benefit Australia, and any possible assistance they can provide from their offices in achieving shared objectives.

2. **Work with Government Ministries and ASQA and expedite the process of regulation of an Australian RTO, as well as gaining accreditation and subsidies for proposed new courses in specialized cyber security roles.** Roles that are essential for growth and Australia's VET programs do not currently have on offer.

3. **Receive Support from the Department of Education to export our programs through Australian Universities Continuing Education Departments, as non-award, non-accredited, expedited training boot camps.** Giving working knowledge to students looking to re-skill or up-skill to enter the cyber security workforce.

4. **Join together with government initiatives such as AustCyber,** helping one another with industry and academic contacts, and consulting with them about how we can use our innovative education system to directly benefit the Australian cyber-ecosystem.

Conclusion

By all official accounts, Australia's cyber security industry faces a shortage of skilled workers. Using only official data, at low estimates in ten years, the current trajectory of the education system will not be able to keep pace with the growing demand.

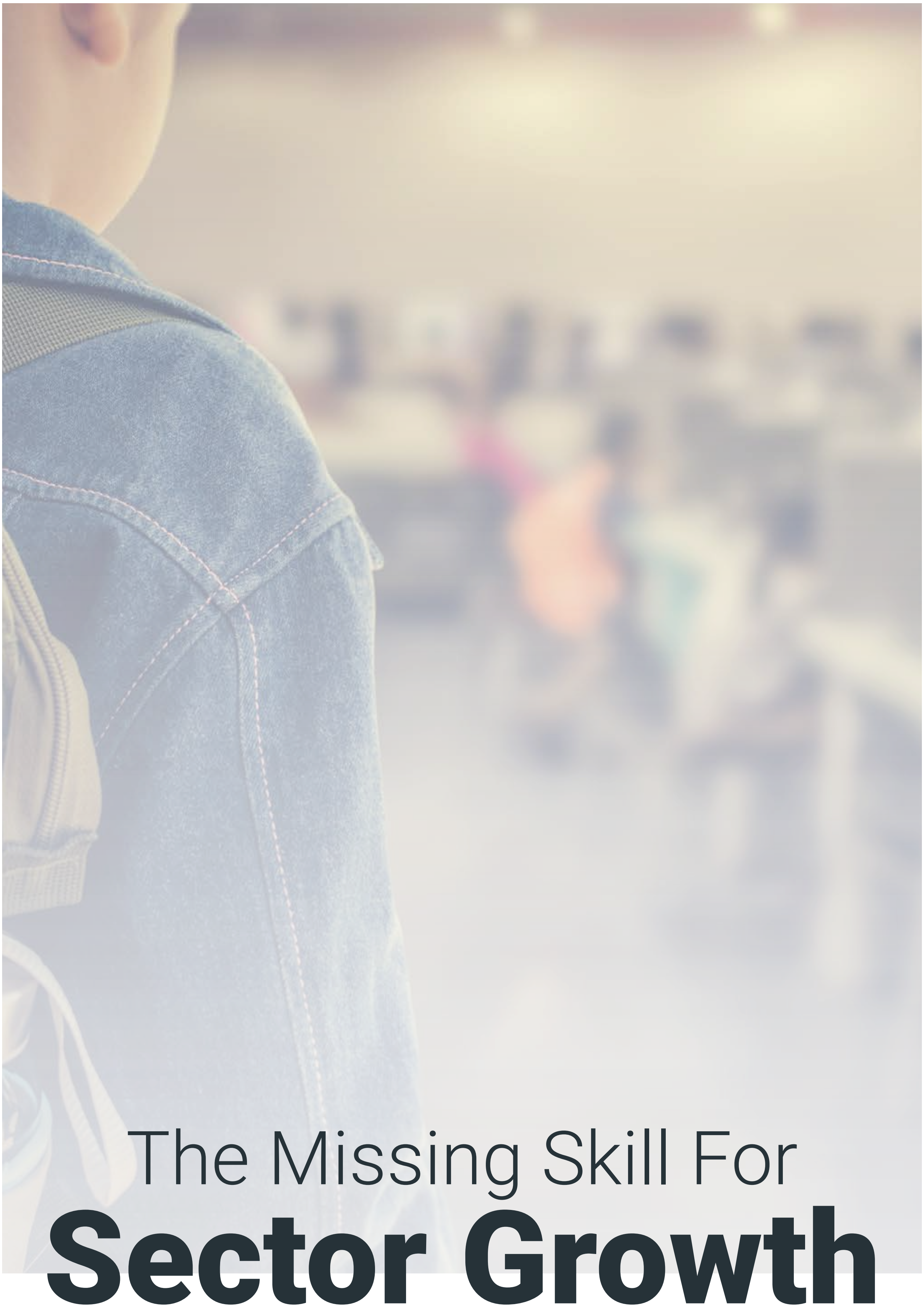
This shortage of skilled workers increases salaries to a point where it's impractical to hire an in-house team for 95% of Australian businesses. The shortage impacts cyber security innovation, and industry and leaves Australia behind its peers in one of the most important industries of the future.

Aside from the direct economic benefits of being able to supply a large cyber security workforce, the indirect advantages of Australia's digital transformation are made clear in the referenced reports.

The relevant Australian authorities can look at this approach in trading with Israel, as perhaps one of the most beneficial ways of working together.

The Teach a Man to F.I.S.H. Initiative offers Australia the opportunity to utilize the core innovations which have given Israel it's an edge to develop the vast array of cyber security products and services that currently dominate the international market.

Leveraging the creation of skilled labor in Australia, rather than simply buying the fruits of that labor from foreign countries strengthens Australia, and may prove to be one of the most important trade initiatives proposed between Israel and Australia.



The Missing Skill For Sector Growth

Technical Course Comparison

Technical Course Comparison

CONTRIBUTORS

Authored By:

Jesse Miller

Head Of International Development & Government Relations

HackerU Global Education

Jessem@hackeru.com
+972.50.222.4978

Technical Audit:

Swaroop Yermalkar

Cyber-Security Content Developer & Instructor

HackerU International - India Division

Swaroop@hackeru.com

Technical Audit Review:

Idan Stambulchik

Head Of Cybersecurity Development

HackerU Solutions

Idan@hackeruso.com

Table Of Contents

Preface

1. The purpose of this document is to demonstrate that the Training Packages and Cybersecurity Courses currently available to the Australian Public have learning outcomes distinct from HackerU's proposed course in Offensive Cybersecurity.

2. We have made our developed evidence based on available documents. Evidence used will address the vastly different ICT training package and an example qualification, and the two courses which are relevant, and widely available to the public.

3. The Qualification used to demonstrate the irrelevance of the ICT training package in the proposed course is:
    a. ICT20120

4. The Courses used for a unit by unit technical comparison are:
    a. 22334VIC
    b. 22445VIC

5. These courses are of a vastly different level of qualification. Class IV vs. Advanced Diploma respectively.

6. Despite the disparity in subject complexity, hours of study, and units of more competency, The available cybersecurity courses do not meet the needs of the learning objectives proposed herein.

7. The Evidence provided for this document was collected by highly credentialed professionals in cybersecurity. Both in education and development.

8. The review was meticulous and conducted by 2 highly credentialed cybersecurity experts.
    a. One Expert in the area of Offensive Cybersecurity the proposed course (See Appendix D)
    b. One Expert in the area of Defensive Cybersecurity (See Appendix E.)

9. The review methodically evaluates all currently accredited units of competency. Both Core and Electives

10. After a thorough examination of all units in the publically available Cybersecurity Courses, the conclusion was that there are no possible combinations of units of competency which can meet the learning outcomes equivalent, or significantly comparable, to those of HackerU's proposed course.

11. HackerU's proposed course addresses the gap between required skills for current industry demand with its curriculum.

12. This document, along with the evidence of the skills shortage (Industry Demand) and the Evidence of Student Demand (Student Forecast), will prove that it is in the public's interest to grant HackerU permission to apply for the accreditation of a **Class IV Certificate in Offensive Cybersecurity**.

Background

General

1. Cybersecurity is an essential skill set for the global economy.

2. It is estimated that Australia has lost Trillions due to cyber-attacks and cyber-crime. Companies require robust defenses.

3. The cybersecurity industry is one of the fastest-growing industries worldwide. Products and services protecting companies from cyber-threats are currently a multi-billion dollar industry.

4. The Cybersecurity industry will grow exponentially in the coming years as more businesses begin to completely rely on the online economy.

5. To create these products and services, and the industry that supports them, two kinds of cyber-security experts are required.

6. One of the essential skill-sets would be a “Defensive Cybersecurity Expert” - (referred to in the cybersecurity industry colloquially as *Blue Team*) This skill set entails identifying potential threats and using current methods to thwart them.

7. The other essential skill set, and the skill set proposed herein, is “Offensive Cybersecurity” (Referred to in the cybersecurity industry colloquially as *Red Team*) This skill set requires experts to test systems for potential entry points and to identify weaknesses with the aim of creating new defensive tools and protocols.

Skills Gap Impact On Industry And Government

8. While a massive skilled labor shortage exists for Defensive “Blue Team” Qualifications, the skill set’s Offensive “Red Team” counterpart is just as essential and has an even more severe shortage.

9. Industry is often relying on specialized firms to deliver this essential “Red Team” service. Due to the extreme lack of qualified professionals, the price for such services is astronomically high and unaffordable for many emerging and growing cybersecurity companies.

10. The skills shortage prevents many overseas cybersecurity conglomerates from setting up technical operations in Australia which further diminishes the availability of current skill sets and experience.

11. It slows the emergence of venture capital firms willing to invest in the cybersecurity sector locally, and stunts the growth of the domestic cybersecurity sector broadly in Australia,

12. Because of the skills gap and correlated pricing of services, essential systems testing is unavailable to many small online companies as well as many medium-sized companies.

13. In an increasingly digital and international marketplace, this can severely lessen a competitive advantage. Large companies often elect to hire temporary contractors which leaves an essential part of the company's cybersecurity apparatus unattended to and substantially less secure.

14. Perhaps most importantly, Government institutions and critical infrastructure require the availability of these professionals. Due to the worker shortage, and the need to compete with private-sector salaries, Australian Government budgets must be increased substantially.

15. This can cause an undue burden on the Australian Taxpayer if the skills gap problem is not addressed.

Current Options For Education

16. There are a total listed 4 cybersecurity courses accredited by ASQA, 2 of which are privately owned and did not respond to requests for documentation that could be used for a proper technical comparison.

17. The two courses which do address the cybersecurity skills gap, do little to teach students active measures. The very measures required for even an entry-level position at a cybersecurity firm, or as an in-house cybersecurity employee.

18. Our Technical review has shown that the two courses widely available to the Public through TAFEs and some RTOs do have some defensive cybersecurity elements in them, but focus largely on theory, policy, and compliance rather than practical technical experience which readies students for the job market.

19. Neither of the courses has any combinations of elective units of competency which could be suitable to ready a graduate for work in "Red Team" or Offensive Cyber Security in an entry-level position.

20. Universities may teach courses relevant to competence in Offensive Cyber-security. However, due to the speed that industry needs evolve, a graduate often finds themselves in a situation where his first year of studies is no longer relevant to common industry practices and required knowledge on the day of their graduation.

21. For these reasons, a course is needed which can focus on the current needs of the job market.

22. A specialist course that can ready students for 3rd party professionally recognized industry-standard certifications and can accomplish this task within 1 year.

The Proposal For Accreditation

23. HackerU’s course works on teaching the required background knowledge. An adequate level of knowledge and practical hands-on training to be considered qualified for Defensive work.

24. Yet the proposed course will focus is on the specialized skill set and practical use of current process and methods which qualify graduates to work in Offensive Cybersecurity Active Measures.

25. The majority of course-work uses real-life simulations and scenarios to teach and assess students’ competence.

26. Nearly all the curriculum is aimed at readying graduates for a 3rd party professional certification, the OSCP, which is the accepted standard for competency internationally. HackerU’s graduates are job-ready and attractive candidates to employers.

Supporting Evidence

General ICT Training Package Overview

1. ICT is defined as the following: *"an extensional term for information technology (IT) that stresses the role of unified communications[1] and the integration of telecommunications (telephone lines and wireless signals) and computers, as well as necessary enterprise software, middleware, storage and audiovisual, that enable users to access, store, transmit, and manipulate information.[2]*

   The term ICT is also used to refer to the convergence of audiovisual and telephone networks with computer networks through a single cabling or link system." (Wikipedia - https://en.wikipedia.org/wiki/Information_and_communications_technology)

2. The standard framework for creating and assessing ICT skillsets is SFIA (*Skills Framework for the Information Age*) while the definition of ICT competencies is very broad, the usual theoretical knowledge base and practical application of ICT skills are considered by experts to be significantly different than cybersecurity training.

3. The professions derived from an ICT education and that of cybersecurity training programs are vastly different to the extent that by course learning objectives do not translate. Even graduates of most 4-year ICT degree programs are not proficient in general cybersecurity and surely not a specialized skill set within that area of expertise.

4. The SIFA framework does include cybersecurity, available here: https://sfia-online.org/en/sfia-7/sfia-views/cybersecurity-skills-in-sfia?path=/glance

5. In the internationally accepted SIFA framework, some core concepts relating to cybersecurity, as well as subjects related to the proposed course material are mentioned.

6. However, where mentioned, SFIA considers such skills as "Skills for Security Professionals". The authoritative framework does not consider the skills proposed by this course such as penetration testing, a skill-set that a general ICT worker should know, let alone have proficiency in.

7. In the available course documentation, of both Class IV Certificate in Cybersecurity, and Advanced Diploma in Cybersecurity (assessed in this document) qualifications from the ICT training package are not used.

8. This request is proposing a specialized course under what Australian courses categorize as cybersecurity.

9. If the current ICT package qualifications are not core skill-sets for the current general cybersecurity courses (22334VIC & 22445VIC), there is no possibility for the learning objectives and learning outcomes of the current version of the ICT training package to translate into competency in a specialized skill set of Offensive “Red Team” Cybersecurity.

10. Offensive or “Red Team” cybersecurity is a specialist skill-set under the cybersecurity category. Most training programs in such skills require a base knowledge in cybersecurity as a prerequisite.

11. While the proposed course does involve issues related to ICT - The ICT training package has no possible combination of units of competency that can achieve the learning objectives proposed herein.

12. Please refer to Appendix A. For an example technical review of a qualification from the current ICT training package.

Supporting Evidence - *22334*VIC

Statement Of Distinctions In Learning Outcomes

1. According to our findings, and supported by evidence in Appendix A, 22334VIC course's learning outcomes realistically prepare graduates for competence in policy, compliance, and some theoretical background knowledge in Defensive Cybersecurity.

2. While the 22334VIC covers several concepts of web application security, there are little to no requirements for hands-on, practical skills development. Due to this, and the syllabus more broadly, graduates could not expect a learning outcome of using practical active measures in the cybersecurity field.

3. None of the units of competency of 22334VIC, both core and elective, can be used in any way for a student to gain competence in Offensive Cybersecurity. The proposed learning outcome of HackerU's course.

Points of Contrast In Learning Outcomes

4. HackerU's Proposed Course for Offensive Cybersecurity offers a learning outcome of practical hands-on experience in Offensive Cybersecurity.

5. The Proposed Curriculum is based on requirements suggested by the NIST Cybersecurity Framework for offensive cybersecurity roles. (See Appendix C for proposed course curriculum)

6. See NIST Cybersecurity Framework https://www.nist.gov/cyberframework.

7. HackerU's proposed course prepares students for active measures and real-world scenarios. It prepares students for the OSCP, a 3rd party international standard for offensive cybersecurity competency.

8. See OSCP: https://www.offensive-security.com/.

9. 22334VIC prepares students for competency in compliance and industry norms to protect IT infrastructure. However, it is not designed to prove competency in active measures in Offensive "Red Team" cybersecurity in any part of its curriculum, and there is no combination of elective courses that could achieve that outcome.

10. Further, The professional certifications which HackerU's course prepares students for are often also accepted for Defensive "Blue Team" cybersecurity.

11. 22334VIC would not qualify graduates for any professional roles in active measures in both defensive and offensive cybersecurity by industry-standard requirements or by the NIST Framework.

Summary of Evidentiary Findings Supporting The Proposal

12. As demonstrated in evidence submitted in Appendix A, the 22334VIC course does not have any possible scenario of combinations of electives that could qualify a student for the proposed Offensive Cybersecurity course's learning outcomes.

13. They are different fields, students must be trained using technology not available to students of 22334VIC, and according to our team, using the information available, the existing course learning objectives and outcomes would not be applicable to any role in the Offensive Cybersecurity field in line with the NIST Cybersecurity Framework. (See Appendix B. for technical comparison)

Supporting Evidence - 22445VIC

Statement Of Distinctions In Learning Outcomes

1. According to our findings, and supported by evidence in Appendix A - 22445VIC course's learning outcomes realistically prepare graduates for competence in Information Security Audits, Forensics, and Risk Analysis. All of which are under a Defensive Cybersecurity category designation.

2. 22445VIC builds on the units in 22334VIC and expands upon the concepts. However, its learning outcomes are similar in both courses as are the units of competency the course is comprised of.

3. None of the units of competency of 22445VIC, either core and elective, can be used in any way for a student to gain competence in Offensive CyberSecurity. The proposed learning outcome of HackerU's course

Points of Contrast In Learning Outcomes

4. HackerU's Proposed Course for Offensive Cybersecurity aims at a learning outcome of practical hands-on experience in Offensive Cybersecurity. HackerU's proposed course prepares students for active measures and real-world scenarios. It prepares students for the OSCP, a 3rd party international standard for offensive cybersecurity competency.

5. See OSCP: https://www.offensive-security.com/

6. 22445VIC prepares students for competency in cybersecurity forensics, compliance, and methods of defense.

7. 22445VIC lacks tools and practical hands-on training in how to deal with events for Defensive scenarios. It is not designed to prove competency in active measures in Offensive "Red Team" cybersecurity in any part of its curriculum, and there is no combination of elective courses that could achieve that outcome.

8. Further, The professional certifications which HackerU's course prepares students for are often accepted for Defensive "Blue Team" cybersecurity and go beyond the capabilities of 22445VIC.

Summary of Evidentiary Findings Supporting The Proposal

9. HackerU's Proposed Course for Offensive Cybersecurity offers a learning outcome of practical hands-on experience in Offensive Cybersecurity in line with the suggested requirements of the industry-standard NIST Cybersecurity Framework. (See Appendix C for proposed course curriculum)

10. See NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

11. HackerU's proposed course prepares students for active measures and real-world scenarios. It prepares students for the OSCP, a 3rd party international standard for offensive cybersecurity competency.

12. See OSCP: https://www.offensive-security.com/

13. 22445VIC prepares students for competency in forensics, compliance, and risk analysis.

14. 22445VIC is not designed to prove competency in active measures in Offensive "Red Team" cybersecurity in any part of its curriculum, and there is no combination of elective courses that could achieve that outcome. (See Appendix B. for technical comparison)

Conclusion

1. HackerU's Proposed Class IV Certificate in Offensive Cybersecurity provides in-depth and hands-on knowledge on Offensive Cyber Security Active Measures.

2. HackerU's Course is kept up to date and in line with the international industry-standard NIST Cybersecurity Framework.

3. The proposed course prepares students for the internationally recognized, industry-standard OSCP exam and makes students fit for working in the security industry immediately upon graduation.

4. HackerU's Offensive Cybersecurity course also gives practical security knowledge and attack vectors for the latest technologies such as IoT, Cloud, DevOps, and Docker.

5. The proposed course would be the most advanced Cybersecurity Course out of the current publically available courses in the VET catalog accredited by ASQA.

6. The proposed course has unique learning outcomes, and HackerU would develop all its current course materials as unique units of competency in compliance with the AQF Guidelines.

Appendix

ICT20120

An Example Qualification From The ICT Training Package

Appendix A.

Comparison To ICT Training Package Qualification - Example

Summary

Course Code: ICT20120

Course Name: Certificate II in Applied Digital Technologies

Source Document(s)

https://training.gov.au/Training/Details/ICT20120

Stated Learning Outcomes:

1. This course provides the foundation skills and knowledge to use basic applied digital technologies in varied contexts.

2. The course is designed for those developing the necessary digital and technology skills in preparation for work.

3. The individuals can carry out a range of basic procedural and operational tasks that require digital and technology skills.

4. They can perform a range of mainly routine tasks using limited practical skills and knowledge in a defined context.

Post analysis learning outcomes:

The course focuses on giving basic knowledge on Technologies but it doesn't focus on the technologies needed by personnel to get started in the field of security. It discusses mainly configuration and setting up the working environment but does not focus on securing the work place.

Qualification:

The course focus is on giving basic knowledge on Technologies but it doesn't focus on the technologies needed by personnel to get started in the field of security. It focuses on Health and safety, Operating Data processing software like Word and Spreadsheet. It focuses on the configuration of the hardware device like computer and also it trains students about setting up the communication platform within an Organisation.

However, the course doesn't focus on hands-on training on offensive security or penetration testing. The course doesn't give any knowledge about Penetration testing skills.

The course doesn't focus on advanced topics like Malware Analysis, Infrastructure Attacks, Web Application Penetration Testing, Mobile security and it also doesn't train students in automating the security tasks using scripting languages like Python or Go.

Post-Analysis Comparison:

The course focus is on giving basic knowledge on Technologies but it doesn't focus on the technologies needed by personnel to get started in the field of cybersecurity. It focuses on Health and safety, Operating Data processing software like Word and Spreadsheet. It focuses on the configuration of the hardware device like a computer and also it trains students on setting up the communication platform within an Organisation.

It doesn't train students or make a topic of discussion the security risks that should be taken care of while setting up any hardware devices or communication devices like Email and telephones. Whereas, HackerU's proposed course provides in-depth and hands-on practical training in Offensive Cyber Security Active Measures.

HackerU's Course provides training in an environment that is as close to what is required in the cybersecurity industry as possible. Real-life simulations give the student a place to apply the course's theoretical knowledge on the latest methods of penetrating by Malware Analysis, Infrastructure Attacks, Web Application Penetration Testing, mobile security, Digital Forensics, and Incident Response.

HackerU's course is kept current and prepares graduates for the international standard professional exam, the OSCP, as well as to prove competence to employers on a level suitable for a junior position on a "Red Team" in the cybersecurity industry immediately upon graduation.

Summary:

HackerU's proposed course provides in-depth and hands-on practical training in Offensive Cyber Security Active Measures. HackerU's Course is provides training in an environment that is as close to what is required in the cybersecurity industry as possible.

Real-life simulations give the student a place to apply the course's theoretical knowledge on the latest methods of penetrating by Malware Analysis, Infrastructure Attacks, Web Application Penetration Testing, mobile security, Digital Forensics, and Incident Response.

HackerU's course is kept current and prepares graduates for the international standard professional exam, the OSCP, as well as proving competence to employers on a level suitable for a junior position on a "Red Team" in the cybersecurity industry immediately upon graduation.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
1	BSBSUS211	Participate in sustainable work practices	https://training.gov.au/TrainingComponentFiles/BSB/BSBSUS211_R1.pdf	https://training.gov.au/TrainingComponentFiles/BSB/BSBSUS211_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to measure, support and find opportunities to improve the sustainability of work practices."	This unit trains students on the procedure and functionalities which every employee of an organization must be aware of. It is not related to cybersecurity and also it doesn't train students on any technology which can help them to start a career in the field of cybersecurity.	This unit trains students on the procedure and functionalities which every employee of the organization has to be aware of. It is not related to cybersecurity and also it doesn't train students about any technology which can help them to start a career in the field of security.
2	BSBTEC202	Use digital technologies to communicate in a work environment	https://training.gov.au/TrainingComponentFiles/BSB/BSBTEC202_R1.pdf	https://training.gov.au/TrainingComponentFiles/BSB/BSBTEC202_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to effectively identify, select and use available methods of digital communication in a workplace context. These methods may include email, instant messaging and other similar platforms."	This unit mainly focuses on the use of digital technology to enhance the communication standards in the work environment. It does not train students on the risks coming from Phishing, Vishing and different social engineering attacks.	This unit mainly focuses on implementing communication solutions within the work environment. It does not focus on the risks and precautions to be taken while setting up the email, instant messaging, and other platforms. This will risk the privacy of an organization.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
3	BSBWHS211	Contribute to the health and safety of self and others.	https://training.gov.au/TrainingComponentFiles/BSB/BSBWHS211_R1.pdf	https://training.gov.au/TrainingComponentFiles/BSB/BSBWHS211_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to work in a manner that is healthy and safe in relation to self and others, and to assist in responding to incidents. It covers following work health and safety (WHS) policies, procedures, instructions and requirements; and participating in WHS consultative processes."	This unit discusses Health and Safety and trains for the same. It does not give any technical knowledge which is needed to get started in the field of Cyber-security.	The unit trains students to contribute to the health and safety of the self and others. It is not focusing on security terminologies or methodologies. It will not train the students for any technical concepts.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
4	ICTICT213	Use computer operating systems and hardware	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT213_R1.pdff	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT213_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to select, install, configure and use computer operating systems and basic computer hardware. This involves configuring the operating system to work with a variety of hardware peripherals and types of information and communications technology (ICT) equipment."	1. This unit will mainly train students to "select, install, configure and use a computer operating system", "install, configure and run at least one application software and at least one supporting hardware component"", ""optimize the operating system using tools, drivers and vendor utilities". 2. This unit trains students on hardware configurations, not about security. This unit will not focus on the security implementation of devices and computers. It does not focus on testing the devices for security loopholes.	This unit trains about configuration and System Administration part. It doesn't focus on securing the devices or computers or secure configuration of the devices and computers.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Non-technical)
5	ICTICT214	Operate application software packages	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT214_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT214_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to identify, select and operate commercial software packages, including a word-processing and a spreadsheet application package."	1. This unit mainly trains students on working with Data in Word or a Spreadsheet. 2. This unit is not for security and even it doesn't focus on technologies needed to learn cybersecurity.	This unit focuses mainly on training students to work with data processing software like Word and Spreadsheets. It has nothing to do with Cybersecurity and any other technology which will support entry into the cybersecurity field.
6	ICTICT215	Operate digital media technology packages	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT215_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT215_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to identify, select and use a digital media package and supporting technologies to produce a variety of media rich documents."	1. ""This unit is mainly for Graphic designing, visual design, and digital media technology. "" 2. This unit is not for security and even it doesn't focus on technologies needed to learn cybersecurity.	The unit focuses on "basic principles of visual design,"" functions and features of digital media packages and technologies". The unit is mainly focused on operating digital media technology. The unit is not for training students in cybersecurity or any other technology needed for cybersecurity.

22334VIC

Appendix B.

Technical Audit Findings

Summary

Course Code: 22334VIC

Course Name: Certificate IV in Cyber Security

Source Document(s)

: https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf

Stated Learning Outcomes:

The student will gain knowledge mostly on the Compliance and Defensive Cybersecurity Measures side of security. The course has got a few concepts of web application security covered in the course however there is not much hands-on training.
The outcomes of this course are the following:

1. networking basics required for cyber security

2. IT skills required for cyber security

3. system testing procedures

4. introduction to data collection and analysis

5. securing a web site

6. introduction to cyber security

7. implementing network security

8. managing a cyber security system

9. incident response plans

10. cyber security project.

Post analysis learning outcomes:

The course's focus is on ""monitor the risk of cyber security attacks, implement appropriate software, use a range of tools and procedures to mitigate cyber security threats, protect an organisation from insider security breaches, develop systems to minimise network vulnerabilities and risks""

Qualification:

This course focus on handling the incident (post-attack) in an organization. This course focuses on building policies and designing the security architecture within the organization. This course will also train the learners only on the secure configuration or setting up the environment, and networking devices. This course also includes the basics of Wireless Security, Web Application Security, IoT devices, and monitoring the devices.

Post-Analysis Comparison:

The course mainly focuses on enabling graduates to ""monitor the risk of cyber security attacks, implement appropriate software, use a range of tools and procedures to mitigate cyber security threats, protect an organisation from insider security breaches, develop systems to minimise network vulnerabilities and risks"". The course heavily focuses on what is classified as “Compliance” in cybersecurity.

However, the course doesn't focus on hands-on training on offensive security or penetration testing. The course doesn't give any knowledge about Penetration testing skills. The course doesn't focus on advanced topics like Malware Analysis, Infrastructure Attacks, Web Application Penetration Testing, Mobile security and it also doesn't train students in automating the security tasks using scripting languages like Python or Go.

Summary:

This course's focus is mainly on what would be classified as ""Compliance"" in Cybersecurity as well as some aspects of ""Defensive"" Cybersecurity Measures. This would include basic training in securing security architecture, post-attack forensics, and developing and implementing policy and procedures. While the subjects of Compliance and the basic Defensive Measures taught in this Course are important aspects of cybersecurity, without proper penetration testing or offensive measures, organizations are left unequipped to provide the intelligence necessary even for well trained and experienced defensive cybersecurity personnel to harden security systems, seal exploits, or for graduates of this course to potentially create defensive policies, protocols, and responses, beyond the standard best practices.

Whereas, HackerU’s proposed course provides in-depth and hands-on practical training in Offensive Cyber Security Active Measures. HackerU’s Course is provides training in an environment that is as close to what is required in the cybersecurity industry as possible. Real-life simulations give the student a place to apply the course’s theoretical knowledge on the latest methods of penetrating by Malware Analysis, Infrastructure Attacks, Web Application Penetration Testing, mobile security, Digital Forensics, Incident Response. HackerU's course is kept current and prepares graduates for the international standard professional exam, the OSCP, as well as to prove competence to employers on a level suitable for a junior position on a ""Red Team"" in the cybersecurity industry immediately after graduation.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
1	VU21995	Manage the security infrastructure for the organization.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This Unit's focus is only on the monitoring i.e SOC part of cybersecurity	1. Not related to Offensive Cyber Security Active Measures and real-time penetration testing. 2. In Offensive Cybersecurity, it's important to understand the different attack vectors, possible vulnerabilities, exploitation, lateral movement, etc	This Unit's focus is on monitoring an organization's technology infrastructure for attacks. This provides an alert to the security personnel so that the team would be ready for the attacks coming in their direction. However, this Unit mainly focuses on a Defensive aspect, not on the offensive aspects of cybersecurity. Meaning, this will not train the security personnel from attacks on the organization by finding all the potential loopholes and bugs. Offensive Cybersecurity or "Red Team" personnel would perform the important task of making known to the organization what could be leveraged by a third-party attacker.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
2	ICTNWK509	Design and implement a security perimeter for ICT networks.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK509_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK509_AssessmentRequirements_R1.pdf	1. This unit provides knowledge on tools and methodologies to design the security architecture for an organisation. 2. The unit includes the implementation of a process for reviewing the existing security architecture and to conduct a security design audit to recommend improvements. 3. This would be mainly catagorized as the compliance side of cybersecurity	1. This Unit’s focus is on what would be classified as “Compliance” in cybersecurity and not on Offensive "red team" Tactics. 2. No Hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit's focus is on building policies and designing the security architecture within the organization. However, this unit does not give training or theoretical knowledge in Offensive Cybersecurity Tactics or "Red Team" activities with which future attacks could be avoided.
3	VU21994	Perform basic cybersecurity data analysis.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This Unit’s focus is on Defensive Cybersecurity Measures and Incident Handling in cybersecurity.	This Unit does not include Offensive Cyber Security or hands-on training in Penetration testing. In Offensive Cybersecurity, students must first understand the various attack vectors before securing/preventing them.	This Unit's focus is on Defensive Cybersecurity and will not train students to actively test an organization's security in order to harden the organization's defenses and prevent attacks.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
4	ICTNWK531	Configuring an Internal gateway	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK531_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK531_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to connect network hardware devices, mainly personal computers (PCs), to an internet gateway."	1. This Unit is related to the setup or configuration of Hardware and Networks, not on the active attack vectors. 2. This Unit will give knowledge to students seeking employment as a Network Administrator and not in roles related to Offensive Security. 3. This Unit requires no Hands-on training on Offensive Security or Penetration Testing.	This Unit will train students on the configuration or setting up the networking devices. This will not train the students in probing exploits in the security of the networking devices.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
5	ICTSAS409	Manage risks involving ICT systems and technology	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS409_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS409_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to implement procedures that identify, analyse, evaluate and monitor risks involving information and communications technology (ICT) systems and technology." 2. "This unit includes the development and management of contingency plans." 3. This Unit's focus is only on monitoring i.e SOC in cybersecurity.	1. This Unit's focus is on possible threats and risks associated with the ICT systems but not on the active attack vectors. 2. Not related to Offensive Cybersecurity Active Measures or real-time penetration testing. 3. This Unit does not require Hands-on training on Offensive Cybersecurity or Penetration Testing.	This Unit focuses on Monitoring the organization for attacks. This knowledge could provide graduates with the ability to alert the cybersecurity personnel so that the team would be prepared for potential attacks. However, this Unit mainly focuses on Defensive Cybersecurity knowledge, not on any ""Red Team"" Tactics. Meaning, this will not train the security personnel on finding and exploiting loopholes and bugs in an organization's infrastructure. Using Offensive Tactics, the organization would know potential flaws in cybersecurity beforehand which could be leveraged by a third-party attacker. Allowing them to harden their defenses accordingly.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Non-technical)
6	RIICOM301D	Communicate information.	https://training.gov.au/TrainingComponentFiles/RII/RIICOM301D_R3.pdf	https://training.gov.au/TrainingComponentFiles/RII/RIICOM301D_AssessmentRequirements_R3.pdf	1. "This unit describes a participant’s skills and knowledge required to communicate in the workplace within the Resources and Infrastructure Industries." 2. This Unit's focus would be categorized as ""Compliance"" in cybersecurity.	1. This Unit does not include Offensive Cyber Security or hands-on training in Penetration testing. 2. In the cybersecurity industry, personnel must first understand the various attack vectors before securing/ preventing them.	This Unit focuses on the policies and security architecture of an organization. However, it doesn't train students in how to better secure an organization’s security infrastructure by exploiting or probing loopholes in the system. Security professionals, trained in Offensive Cybersecurity Active Measures, are essential for providing the knowledge about potential weaknesses or risks through their own Penetration Testing. This is required knowledge before an appropriate response plan is developed and communicated to the organization.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
7	VU21990	Recognize the need for cybersecurity in an organization.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This Unit’s focus is on performing a standard vulnerability assessment	1. This Unit does not focus on probing and exploiting vulnerabilities to find existing or new potential weaknesses in security. 2. This Unit requires no hands-on training on VAPT which is expected knowledge in the modern cybersecurity industry.	This Unit only focuses on searching for and finding loopholes in the security system but doesn't train students in any active measures to leverage the loopholes found during the assessment. Where some aspects of this Unit may be applicable to Offensive Cybersecurity, the unit alone or in the context of the whole course would be insufficient for a student to apply their knowledge practically.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
8	VU21988	Utilize basic network concepts and protocols required in cybersecurity.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	Focuses on Basic Network Admin part.	This module can be considered as fundamentals/basics for the Offensive Cyber Security Active Measures. It does not focus on Active Measures a Network Environment.	This module will train the students only on the configuration or setting up of a networking environment. This will not train students to prod weaknesses and find new exploits in the security of an organization.
9	VU21996	Evaluate and test an incident response plan for an enterprise.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This module focuses on Incident Handling, Response, and Defensive Cybersecurity tactics.	This Unit does not actively train in the exploitation of loopholes or probing of an organization's IT security Infrastructure.	This unit’s focus is on Incident Response (scenarios where the hack has already occurred) in an organization. This unit does not train a student in leveraging weaknesses, and because of this, graduates lack practical knowledge or experience in exploiting loopholes that already exist. The ability to do this is essential in preventing attacks from occurring in the first place.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
10	ICTICT418	Contribute to copyright, ethics, and privacy in an ICT environment.	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT418_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTICT418_AssessmentRequirements_R1.pdf	1. This unit describes the skills and knowledge required to maintain professional and ethical conduct. 2. This Unit’s focus would be categorized as ""Compliance"" in cybersecurity.	1. The subject matter in this Unit is not in any way related to Offensive Cyber Security Active Measures and Real-time Penetration Testing. 2. The unit’s focus is on policy-related matters, practical exploitation, or security assessments of the ICT environment. 3. This Unit does not require any hands-on training on Offensive Security or Penetration Testing.	This Unit’s focus is on preparing students for working in compliance matters, it is not related to testing the security of an organization's Technology Infrastructure.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
11	BSBWHS401	Implement and monitor WHS policies, procedures and programs to meet legislative requirements.	https://training.gov.au/TrainingComponentFiles/BSB/BSBWHS401_R1.pdf	https://training.gov.au/TrainingComponentFiles/BSB/BSBWHS401_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to implement and monitor an organization’s work health and safety (WHS) policies, procedures and programs in the relevant work area in order to meet legislative requirements." 2. This Unit’s focus is on what would be classified as “Compliance” in cybersecurity.	1. This Unit's focus is on workplace policies and procedures, Not how or in what way it could be exploited. 2. This Unit does not require any hands-on training on Offensive Security or Penetration Testing.	This Unit's focus is on the policies and security architecture of the organization. It has no relevance to testing the infrastructure. It is not understood by the assessor if this course is necessary for learning in Australia. However, when developing policies, Offensive Cybersecurity tactics are used to understand the IT infrastructure's weaknesses and vulnerabilities for which any cybersecurity policy would be created or modified to protect against.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
12	VU21997	Expose website security vulnerabilities.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This Unit's focus is on a very basic OWASP vulnerabilities overview	1. This Unit does not cover web application security in-depth or as hands-on practical training. 2. This Unit does not focus on the manual exploitation of vulnerabilities. The focus is on tools that at times can give false-positive results. 3. Relying only on tools is insufficient as a cybersecurity professional and does not meet standards expected by most employers or organizations today	This module focuses on giving an overview of web vulnerabilities but doesn't go in-depth into each of the potential vulnerabilities or loopholes of a web application. This Unit's focus is on common cybersecurity tools. Manually leveraging exploits and loopholes is important because tools give false-positive results at times. Manual testing is expected knowledge in a cybersecurity role.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
13	ICTSAS418	Monitor and administer security of an ICT system	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS418_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS418_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to monitor and administer security functions of an information and communications technology (ICT) system." 2. This focuses solely on monitoring i.e SOC part of security.	1. This Unit covers a topic that is more of a defensive mechanism. However, it’s essential to understand the attack vectors in order to prevent them effectively. 2. This Unit does not require any hands-on training on Offensive Security or Penetration Testing.	This Unit's focus on Monitoring the organization for attacks. This would prepare graduates to alert the cybersecurity personnel so that the team would be ready for incoming attacks. This module focuses on a defensive aspect of cybersecurity and not on any Offensive Active Measures. This means the Unit does not provide training to students on ethical hacking practices so that all the loopholes and bugs could be already known to an organization, allowing them to develop appropriate Defensive Measures, Protocol, and Policy (the very things this course relates to).

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
14	ICTNWK502	Implement secure encryption technologies.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK502_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK502_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to ensure secure file encryption is selected, implemented and monitored on a computer network or local environment."	1. This Unit's focus is on the implementation of encryption but not on the various attack vectors on encryption or cryptography attacks. 2. The Unit does not require any hands-on training on Offensive Security or Penetration Testing.	This Unit focuses on setting up encryption or a cryptography mechanism but it does not discuss potential loopholes or attack possibilities in cryptography. It's not relevant for any practical measures in offensive cybersecurity.
15	VU21989	Test concepts and procedures for cyber security.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This module touches the topics at the surface level	1. This Unit does not give much in depth and hands-on knowledge about the core cybersecurity concepts as vulnerability assessment, exploit development, malware analysis etc. 2. This Unit doe not discuss the latest and most severe attacks like EternalBlue, Dirty Cow, Lateral movement etc	This Unit gives an overview and does not give in depth theoretical knowledge or any practical training about cybersecurity concepts.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
16	VU21993	Secure a networked personal computer.	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	1. This module focuses on best security practices for a PC network within an organization. 2. This would be classified as basic knowledge in Defensive Cybersecurity.	This Unit does not require students to learn about any possible attack vectors against the personal computer	This Unit discusses best practices when configuring a PC system in the workplace. It does not focus on potential threats to said system.
17	BSBRES401	Analyse and present research information.	https://training.gov.au/TrainingComponentFiles/BSB/BSBRES401_R1.pdf	https://training.gov.au/TrainingComponentFiles/BSB/BSBRES401_AssessmentRequirements_R1.pdf	1. "This Unit describes the skills and knowledge required to gather, organise, analyse and present workplace information using the available systems." 2. This Unit's focus would be classified as ""Compliance"" in cybersecurity\	1. This Unit is not related to Offensive Cyber Security Active Measures and real-time penetration testing. 2. This Unit does not require Hands-on training on Offensive Security or Penetration Testing.	This unit discusses policies as it relates to the security architecture of an organization. It doesn't discuss exploiting the infrastructure, which is a required part of cybersecurity to prevent attacks in an organization, and for cybersecurity tools development.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
18	ICTPRG405	Automate processes.	https://training.gov.au/TrainingComponentFiles/ICT/ICTPRG405_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTPRG405_AssessmentRequirements_R1.pdf	This unit describes the skills and knowledge required to write scripts to automate solutions, by using basic scripting processes, and application-specific scripting options.	1. This Unit's focus is on automating the process but no mention of penetration testing using scripts. 2. This unit only focuses on Bash scripting but not Python/Go Scripting which is in high demand and the current industry standard for cybersecurity professionals.	This Unit gives a basic overview of programming fundamentals but doesn't go in-depth or give advanced knowledge or practical training in scripting. This module doesn't train in Offensive Cybersecurity using scripting.
19	ICTNWK511	Manage network security.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK511_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK511_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to implement and manage security functions throughout a network." 2. This Unit’s stated learning objectives are useful for Network Administrator.	1. This Unit's focus is on configuring secure networks but not on testing for vulnerabilities in the Network Environment. 2. This Unit does not require hands-on training on Offensive Security or Penetration Testing.	This Unit will train the students on the configuration or setting up a secure networking environment. This will not train students in finding vulnerabilities in a networking environment.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
20	VU21991	Implement network security infrastructure for an organisation	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This Unit's focus is on best security practices for Networking and Firewall Security.	1. This Unit does not focus on Offensive Cyber Security Active Measures or advanced infrastructure attacks. 2. This subject matter would be classified as ""Compliance"" in cybersecurity	This Unit’s focus is on best security practices that can be used by the administrators for configuring or setting up the networking environment. It gives no theoretical knowledge or hands-on training in Offensive Cybersecurity measures.
21	VU21992	Develop a cyber security industry project	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/curr22334VICCyberSecurity.pdf	This Unit's focus is on SOC i.e Handling the incident.	1. This Unit does not give theoretical knowledge or practical training in real-time exploitation testing. 2. This Unit does not cover threat hunting or threat intelligence.	This Unit's focus is on handling an incident (on-going, or previous hack) in an organization. It doesn't train the student for finding weaknesses and testing exploits that could have prevented the hack from having occurred in the first place.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Non-technical)
22	ICTNWK416	Build security into virtual private networks.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK416_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK416_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to build security into a virtual private network (VPN)." 2. This Unit’s stated learning objectives are useful knowledge for a Network Administrator.	1. This topic doesn’t discuss possible attack vectors against the virtualized environment or the dockerized systems. 2. No Hands-on training on Offensive Security or Penetration Testing.	This Unit’s focus is on best security practices that can be used by the administrators for configuring or setting up the networking environment. It has no practical application to Offensive Cybersecurity Active Measures, which would test the networking environment.
23	ICTPRG407	Write script for software applications.	https://training.gov.au/TrainingComponentFiles/ICT/ICTPRG407_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTPRG407_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to plan, design and build scripts, using a scripting language to construct a highly interactive and automated software application."	1. This Unit’s focus is on automating the process but no mention of penetration testing using scripts. 2. This unit does not discuss scripting with Python or Go which is one of the most used programming languages in the Cybersecurity Industry.	This unit gives a basic overview of programming fundamentals but doesn't go in-depth, nor give advanced knowledge of scripting to standard industry requirements to work in the field. This module doesn't train students in using scripting or automating the security tasks using scripting.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
24	ICTSAS505	Review and update disaster recovery and contingency plans.	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS505_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS505_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to analyse the impact of the system on the organisation and carry out risk analysis, disaster recovery and contingency planning." 2. This Unit's focus would be categorized as ""Compliance"" in cybersecurity.	1. This Unit’s stated learning outcomes are not related to Offensive Cyber Security Active Measures and real-time penetration testing. 2. This Unit discusses preventing and checking the status of security architecture within the environment but not on getting into the organization. 3. This Unit does not require hands-on training on Offensive Security or Penetration Testing.	This unit discusses the policies and security architecture of the organization. It doesn't discuss finding weaknesses in the infrastructure. Cybersecurity personnel, if trained in Offensive Measures would be helpful for developing security policies specific and unique to the organization’s needs and infrastructure.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
25	ICTNWK401	Install and manage a server.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK401_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK401_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to install and manage a server." 2. "Server management includes initial configuration and testing, ongoing administration, software distribution and updates, profiling and monitoring servers, and troubleshooting."	1. This Unit's focus is on the setup/installation of the server but will not cover active attack vectors against the installed server. 2. This unit does not require hands-on training on Offensive Cybersecurity or Penetration Testing.	This Unit focuses on setting up the Server-Client Architecture for an organization but it doesn't discuss attack possibilities or criteria which a professional must be aware of while setting up the environment. Also, this Unit does not discuss the basics of breaking methodology which every administrator should know in order to prevent future security threats to the organization.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
26	ICTNWK503	Install and maintain valid authentication processes.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK503_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK503_AssessmentRequirements_R1.pdf	1. "This course describes the skills and knowledge required to design, develop, install and maintain authentication processes to reduce the vulnerability of the system." 2. This Unit teaches Defensive Cybersecurity "Blue team" aspects in cybersecurity work.	1. It is basically just a configuration and setup of the authentication process i.e mainly a job role of a Network Administrator. It doesn’t cover any topics on attacking the authentication or finding vulnerabilities. 2. This Unit does not require hands-on training on Offensive Security or Penetration Testing.	This Unit focuses on setting up the authentication process and designing the authentication process. It does not train the students on security threats, which they should be aware of while setting up such mechanisms. Knowing the possible security threats is required for an organization to be more secure and less prone to attacks.

22445VIC

Summary

Course Code: 22445VIC

Course Name: Advanced Diploma of Cyber Security

Source Document(s):

https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf

Stated Learning Outcomes:

The student will gain knowledge mostly on the Compliance and Defensive Cybersecurity Measures side of security. This course can allow students to prove competence in aspects of what would be classified as ""Defensive"" Cybersecurity

"Graduates of the Advanced Diploma will have:

- Cognitive and communication skills to identify, analyse and act on cyber security risks, threats and incidents in an organisation.

- Cognitive and communication skills to transfer knowledge and skills to others concerning cyber security risks in workplace practices.

- and to demonstrate specialised knowledge in mitigation strategies.

- Cognitive and communication skills to formulate responses to complex cyber security problems such as protecting critical infrastructure.

- Wide-ranging specialised technical, creative or conceptual skills to express ideas and perspectives on compliance issues and design methodologies to improve an organisation's cyber security."

Post analysis learning outcomes:

This course's focus is on Threat Handling, SOC, and Compliance side of security. The course also covers a few concepts of Web Application Security.

"A summary of the knowledge and skills outcomes of this course are as follows:

• manage and maintain cyber security in an organisation which includes:

- monitoring the risk of cyber security attacks

- gathering, analysing and interpreting threat data

- protecting critical infrastructure and configuring security devices

- evaluating and implementing appropriate security software

- implementing and using a range of tools and procedures to mitigate cyber security threats

- protecting an organisation from insider security breaches

- developing systems to minimise network vulnerabilities and risks

• coordinate security projects which could include both internal and external expertise and resources

• ensure an organisation's security policies, processes, procedures and codes of practice are consistent and inline with relevant security standards, laws and codes of practice."

Qualification:

This course focus on handling the incident(already happened attacks) in an organization. This course focuses on building policies and designing the security architecture within the organization.

This course will also train the learners only on the secure configuration or setting up the environment, networking devices, and virtual environment.

This course also focuses on the basics of Wireless Security, Web Application Security, IoT devices, and monitoring the devices.

Post Analysis Comparison:

The course mainly focuses on ""performing a security risk assessment for an organization", "implementing best practice for identity management", "evaluating an organization's compliance with relevant cyber security standards, laws and codes of practice", "evaluating and implementing security protection devices and software", "managing a cyber security environment", "assessing and securing cloud services", "performing digital forensic investigations on workstations and mobile devices"".

The course also focuses on compliance side of security. But the course does not focus on hands-on training of Red teaming and offensive security. The course does not give knowledge about Penetration testing skills.

The course does not focus on advanced topics like Malware Analysis, Infrastructure Attacks, Cyber Infrastructure, Web Application Penetration Testing and mobile security and it also doesn't train about automating the security tasks using scripting language like Python or Go.

Summary:

This course focuses mainly on what would be classified under ""Forensics"" and ""Compliance"" in cybersecurity. The course doesn't provide hands-on training in practical methods of Offensive cybersecurity such as Penetration Testing to expose exploits and loopholes. For this reason, the course is significantly different than the proposed Course of Offensive Cybersecurity by HackerU

Whereas HackerU's proposed course provides in-depth and hands-on practical training in Offensive Cyber Security Active Measures. HackerU's course offers training in an environment as close to what is required in the cybersecurity industry as possible. Real-life simulations give the student a place to apply for the course's theoretical knowledge on the latest methods of penetrating the newest infrastructure, such as Web Applications, Mobile, and Infrastructure. HackerU's course is kept current and prepares graduates for the international standard professional exam, the OSCP, and proves competence to employers on a level suitable for a junior position on a ""Red Team"" in the cybersecurity industry immediately after graduation. Also, HackerU providing a cloud platform for the students, which calls Cywar, and the students can have hands-on experience in real scenarios.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
1	VU22240	Communicate cyber security incidents within the organisation.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	"This unit provides the knowledge and skills for a learner to communicate the effects of cyber security incidents to appropriate personnel in the organisation."	1. This Unit does not focus on the practical implementation of handling the incident. 2. The Unit is required to teach theoretical knowledge but is not required to train students in practical measures.	This Unit's focus is on Incident Response (ongoing hacks, or post-attack) in an organization. This unit does not train the student in leveraging weaknesses, and because of this, graduates lack practical knowledge or experience in exploiting loopholes that already exist. The ability to do this is essential in preventing attacks from occurring in the first place.
2	VU22241	Interpret and utilise key security frameworks, policies and procedures for an organisation.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	This Unit's focus would be categorized as "Compliance" in cybersecurity security i.e policies, security frameworks, and procedures that are required to build security standards, policies, and protocol within an organization.	1. This Unit would not relate to Offensive Cyber Security Active Measures. 2. This Unit is not required to train to handle incident response	This Unit's focus is on building policies and designing the security architecture within the organization. This is not directly related to training in Offensive Cybersecurity - which policies, protocols, and all other compliance matters should be based on.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
3	VU22242	Assess and secure cloud services.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	This Unit expands on Defensive Cybersecurity Measures i.e On preventing the data on cloud and auditing.	The Unit does not focus on finding the vulnerabilities in Cloud systems.	This Unit's focus is on defending the data in a cloud environment but it does not give any knowledge about possible security loopholes that can help to make the defense accurately related to the potential breach.
4	VU22243	Develop software skills for the cyber security practitioner.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. This Unit focuses on writing secure code. 2. This Unit covers mainly two vulnerabilities i.e Buffer Overflow and SQLi.	"1. This Unit does not require any hands-on training in finding vulnerabilities in code. 2. Web Application security has many other important vulnerabilities which are industry standard knowledge for even the most entry-level role in cybersecurity.	The unit mainly focuses on writing secure code to avoid script kiddies from exploiting it. It does not train the student in exploit testing of the code which helps the coder to understand vulnerabilities and mitigate the possible threats to the product.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
5	VU22244	Implement best practices for identity management.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	This Unit's focus is on Best Security Practices for Administration and on Defensive Cybersecurity Measures.	This Unit does not offer any training related to Offensive Cyber Security Tactics.	This Unit will train students only on the secure configuration or setting up an Environment. This will not train students to probe the exploits of environments. Knowing the possible threats is key to make the organization less prone to cyber-attacks.
6	VU22245	Plan and implement a cyber security project.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	This Unit's focus would be classified as "Compliance" in cybersecurity i.e planning the policies for cybersecurity projects, and SOC.	This unit offers no teaching about Offensive Cyber Security Active Measures and hands-on training on Pentesting the Environment.	This Unit focuses on building policies and designing the security architecture within an organization but it does not train students on the offensive measures from which these policies are developed.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
7	VU22246	Evaluate an organisation's compliance with relevant cyber security standards and Law.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	This Unit's focus would be classified as "Compliance" in cybersecurity (i.e Cyber Security Standards of Projects within an Organization) as well as laws and regulatory guidelines related to cybersecurity.	1. This Unit requires no hands-on training in active measures and is mainly theoretical 2. This module is not related to work in Offensive Cybersecurity Active Measures.	This Unit is focused on building policies and designing the security architecture within the organization but this does not train in probing exploits or penetration testing. On the basis of which future attacks could be prevented.
8	VU22247	Acquire digital forensic data from workstations.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. This Unit's focus is mainly on digital forensics. 2. The Unit focuses on the investigation after the attack has already occured.	This Unit's learning objectives are different from offensive security and don't focus on probing the network or finding and testing exploits in the environment.	This Unit trains students to respond and investigate post-incident. This will not train students to probe the exploits of environments. Knowing the possible threats is key to make the organization less prone to cyber-attacks.
9	VU22248	Acquire digital forensic data from mobile devices.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. This Unit is Digital Forensics oriented training. 2. This Unit focuses on training the student for investigation post-incident.	This Unit's learning objectives are different from offensive security and don't focus on probing the network or finding and testing exploits in the environment.	This Unit trains students to handle and investigate an incident that has already occurred. This will not train students to probe the exploits of environments. Knowing the possible threats is key to make the organization less prone to cyber-attacks.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
10	VU22249	Perform a security risk assessment for an organisation.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	This Unit's focus is on vulnerability assessment	This unit does not focus on exploiting the vulnerability if found which is essential to develop the response.	This unit focus on finding and searching for the loopholes in the security system but doesn't train the student to leverage the loopholes found during an assessment.
11	BSBWOR502	Lead and manage team effectiveness	https://training.gov.au/TrainingComponentFiles/BSB/BSBWOR502_R1.pdf	https://training.gov.au/TrainingComponentFiles/BSB/BSBWOR502_AssessmentRequirements_R1.pdf	“This Unit's objectives are to teach the student "the skills and knowledge required to lead teams in the workplace and to actively engage with the management of the organisation."	1. This Unit is theoretical knowledge about managing a team but nothing related to Offensive Cybersecurity. 2. This Unit does not give practical hands-on training in Offensive Cybersecurity "Red Team" tactics.	This Unit is mainly focused on the management skills needed to lead a security team but this Unit does not require professional training on security threats. Without the practical knowledge of both "Blue Team" and "Red Team" - a graduate would not be qualified for management of a cybersecurity team, making this unit redundant for the purposes of professional training.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Non-technical)
12	ICTNWK525	Configure an enterprise virtual computing environment	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK525_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK525_AssessmentRequirements_R1.pdf	This Unit's objective is to teach students about the skills and knowledge "required to develop and implement virtualisation technologies, with the goal of providing a more sustainable information and communications technology (ICT) environment."	1. This Unit's objective goal to teach about Virtualization but has no concepts of how it may relate to Offensive Cybersecurity. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit gives the ability to set up and configure a virtual computing environment but this does not train a student in dealing with security threats in order to setup the virtual environment securely.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
13	ICTNWK607	Design and implement wireless network security	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK607_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK607_AssessmentRequirements_R1.pdf	This unit' the skills and knowledge required to "mitigate security threats to a wireless local area network (WLAN) by implementing security standards and policies."	1. This Unit's focus is on the network admin side of cybersecurity and on Blue Team i.e this course gives training on how to prevent the WLAN attack. 2. This Unit does not require hands-on training on Offensive Cybersecurity Tactics. 3. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit mainly gives knowledge about setting up the wireless network securely but this does not train about common Wireless attacks and how to prevent them which makes the environment more prone to cyber-attacks.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
14	ICTNWK531	Configure an internet gateway.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK531_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK531_AssessmentRequirements_R1.pdf	"This unit's objective is to teach the skills and knowledge required to connect network hardware devices, mainly personal computers (PCs), to an internet gateway."	1. This Unit's objectives are to train a student to Configure a secure networking environment which would be some basic skills related to "Defensive" cybersecurity. This course is not directly related to cybersecurity and it doesn’t involve any cybersecurity concepts. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit will train students only on the configuration or setting up the networking devices. This will not train students in Offensive Cybersecurity or related subject matter.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
15	ICTSAS505	Review and update disaster recovery and contingency plans	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS505_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS505_AssessmentRequirements_R1.pdf	"This Unit's objective is to teach the skills and knowledge required to analyze the impact of the system on the organization and carry out risk analysis, disaster recovery, and contingency planning."	1. This Unit is not related to Offensive Cybersecurity "Red Team" tactics or hands-on Penetration Testing. 2. This Unit's subject matter would be classified as "Compliance" in cybersecurity 3. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit discusses the policies and security architecture of an organization. It doesn't teach about probing the infrastructure’s vulnerabilities or exploits. It's the findings from this probing of vulnerabilities that good policy is developed.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
16	ICTNWK502	Implement secure encryption technologies.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK502_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK502_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to ensure secure file encryption is selected, implemented and monitored on a computer network or local environment."	1. This Unit trains students on secure file encryption technologies. It includes nothing as to how it would be related to applying offensive cybersecurity methods in the infrastructure or network. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit's focus is on setting up encryption or a cryptography mechanism. It does not discuss loopholes or attack possibilities in cryptography.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
17	ICTNWK503	Install and maintain valid authentication processes	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK503_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK503_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to design, develop, install and maintain authentication processes to reduce the vulnerability of the system." 2. The objective of this unit would be classified as "Defensive" Cybersecurity.	1. The Unit's objective is to teach basic configuration and setup of the authentication process. This is mainly a role for a Network Administrator. It does not cover any topics on probing exploits in the authentication or finding vulnerabilities. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This module focuses on setting up the authentication process and designing the authentication process. But this does not train the learners about security threats which they should be aware of while setting up such mechanisms. Knowing the possible security threats helps the organization to be more secure and less prone to attacks.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
18	ICTSAS501	Develop, implement and evaluate an incident response plan.	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS501_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTSAS501_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to develop and implement an incident response plan." 2. This Unit trains a student for an incident response which would be classified under "Defensive" cybersecurity.	1. This Unit covers an incident response module which is done after an attack has already occurred. The Unit does not teach about Offensive Cybersecurity. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit's focus is on handling the incident (post-hack) in an organization. It doesn't include professional training for offensive tactics which is the basis for protecting an organization from being attacked and is the basis for developing preventative cybersecurity products and services.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
19	ICTNWK513	Manage system security.	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK513_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK513_AssessmentRequirements_R1.pdf	1. "This unit describes the skills and knowledge required to implement and manage security on an operational system. 2. This will help to implement and managing the organization’s security management system."	1. The training offered in this Unit relates to managing the security system and includes nothing about Penetration Testing. 2. No technical aspects of this Unit are related to probing the IT infrastructure. 3. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit gives knowledge about managing the security of the system but this does not teach about possible security loopholes or threats, or how to test them, all subjects which an administrator should be aware of in order to make the system less prone to cyber-attacks.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
20	ICTNWK509	Design and implement a security perimeter for ICT networks	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK509_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTNWK509_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to build a high performance, high security, failure resistant security perimeter, for an enterprise information and communications technology (ICT) network."	1. This Unit's focus is on hardening the security infrastructure of an organization. 2. Pentesting is an essential element to hardening the security of infrastructure but it is not covered in this Unit. 3. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This module focuses on building policies and designing the security architecture within the organization but this does not train in Offensive Cybersecurity with which future attacks could be prevented.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
21	ICTTEN811	Evaluate and apply network security.	https://training.gov.au/TrainingComponentFiles/ICT/ICTTEN811_R1.pdf	https://training.gov.au/TrainingComponentFiles/ICT/ICTTEN811_AssessmentRequirements_R1.pdf	"This unit describes the skills and knowledge required to evaluate security of information communications technology (ICT) networks, using converging switching and transmission technologies in local area networks (LAN) and wide area networks (WAN), broadband networks, internet protocol TV (IPTV) and virtual networks."	1. This Unit's focus is on Administration. Training a network admin to securely configure a network environment. but no focus is on probing exploits to get into the environment, an essential part of creating a secure system. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit will train students only on the configuration or setting up a secure networking environment. It will not train students to test the security of an organization. Nor does it discuss possible security threats that could be used to harden the security system of the environment.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
22	VU22250	Respond to cyber security incidents	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. This unit trains students in Incident Response and Incident Handling. 2. This helps learners for a SOC job profile.	The Unit requires no Offensive Cyber Security Active Measures and hands-on training on Pentesting the environment.	This unit's focus is on handling the incident (ongoing, or post-attack) in an organization. This will not train students to probe the exploits of environments. Knowing the possible threats is key to make the organization less prone to cyber-attacks.
23	VU22251	Gather, analyse and interpret threat data.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. This Unit will train students for setting up hardware and software tools for detecting incidents. 2. This Unit's stated learning outcome would be classified as SOC related in cybersecurity.	This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit provides insights about setting up hardware and software tools in order to detect the threat within an organization but it doesn't give knowledge about probing the security in place. It also doesn't prepare students for manual identification of threats.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
24	VU22252	Implement cyber security operations.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "The unit provides the knowledge and skills to implement and monitor a cyber security operation for an organisation." 2. "The unit also includes the use of tools and processes to analyse data and detect intrusions."	1. This Unit does not focus on probing the security of the environment, just hardening the security infrastructure of the organization. 2. Offensive Security Pentesting is probing the security of an Infrastructure. 3. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit's focus is on monitoring the organization for attacks. The student would be competent to provide an alert to the security personnel so that the team would be ready for incoming attacks. However, this Unit's focus is on what would be classified as "Defensive" Cybersecurity and not Offensive Cybersecurity. This Unit will not train students in testing the security of the organization so that all the loopholes and bugs would be readily known to the organization and could not be leveraged by a third-party attacker.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
25	VU22253	Undertake penetration testing of the security infrastructure for an organisation	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "This unit provides the knowledge and skills required to use a series of tools to test the vulnerabilities of the security infrastructure for an organisation." 2. "The unit includes the compiling of information on the existing security infrastructure design, evaluating and selecting testing tools, and performing vulnerability scanning and penetration testing."	1. This Unit's focus is on tools and does not cover a manual approach. Tools at times give false-positive results and verify that the manual approach is necessary which is not given in this course. 2. This Unit does not focus on the manual exploitation of vulnerabilities. The focus is on tools that at times can give false-positive results. 3. Relying only on tools is insufficient as a cybersecurity professional and does not meet standards expected by most employers or organizations	This module focuses on giving an overview of web vulnerabilities but doesn't go in-depth into each of the potential vulnerabilities or loopholes of a web application. This Unit's focus is on common cybersecurity tools. Manually leveraging exploits and loopholes is important because tools give false-positive results at times. Manual testing is expected knowledge in a cybersecurity role.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
26	VU22254	Undertake advanced penetration testing for web site vulnerabilities.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "This unit provides the knowledge and skills to expand the testing capability for web vulnerabilities." 2. "It also includes the development of a penetration (PEN) test report which will identify the root cause of the issues and includes mitigation strategies for the identified web site weaknesses."	1. This Unit does not cover anything related to Active Directory Pentesting and Reverse Engineering which are an integral part of Offensive Cybersecurity. 2. This Unit focuses on OWASP vulnerabilities but web application security entails many more subjects and has a broad scope. All required knowledge to work in an Offensive role in Cybersecurity	This Unit gives knowledge on Web Application Security and possible loopholes. This Unit does not have any requirements to teach about Mobile or Infrastructure security which is the most integral part of any practical application and needs to be prevented as a priority.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
27	VU22255	Evaluate threats and vulnerabilities of Internet of Things (IoT) devices.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "This unit provides the knowledge and skills to examine the function and operation of IoT devices and to identify what threats and vulnerabilities exit when using them." 2. "The unit also includes strategies to minimise the threats."	1. This unit doesn't focus on Red teaming tactics and Penetration testing concepts. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit gives knowledge about possible security attacks in IOT technology. It does not present practical methods for testing the security of IoT, and does not teach different new technologies like Cloud, Docker, etc in any capacity.
28	VU22256	Protect critical infrastructure for an organisation	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "The units cover the development of mitigation strategies to protect an organisation's infrastructure as well as the implementation and monitoring of its effectiveness." 2. This Unit teaches what is classified as "Compliance" in cybersecurity	1. This Unit focuses on compliance and not on the Offensive "Red Team" tactics. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This Unit teaches policies and security architecture of the organization. It doesn't train students in methods to test and secure the infrastructure.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
29	VU22257	Configure security devices for an organisation.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. This unit covers the secure configuration of security devices. 2. "After implementation the devices will be monitored and assessed for their effectiveness."	1. This unit mainly focuses on configuration but not on the penetration of security infrastructure. 2. This unit doesn’t focus on Red teaming tactics. 3. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This module focuses on setting up security devices for an organization but it doesn't train about the security loopholes in the security devices.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn’t contribute to competency in proposed course learning outcomes	Summary (Not-technical)
30	VU22258	Design and implement a virtualized cyber security infrastructure for an organisation.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "The unit includes designing an infrastructure to suit key specifications, the utilisation of testing procedures in the development stage, implementation process, monitoring functionality following implementation and continuous improvement processes." 2. This Unit’s learning outcomes would be classified as “compliance” in cybersecurity.	1. This focuses on what is classified as "Compliance" in cybersecurity, and not on Offensive, "Red Team" tactics. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit trains students in the policies and security architecture of the organization. It doesn't train students in practical methods of testing and securing the infrastructure.

Sr. No	Unit Code	Name	Unit of Competency	Assessment Requirements	How the unit contributes to competency in stated learning outcomes	How the unit doesn't contribute to competency in proposed course learning outcomes	Summary (Not-technical)
31	VU22259	Utilise design methodologies for security architecture.	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	https://www.education.vic.gov.au/Documents/training/providers/rto/currCyber%20Security%20Advanced%20Diploma22445VIC.pdf	1. "This unit provides knowledge on tools and methodologies to design the security architecture for an organisation." 2. "The unit includes the implementation of a process for reviewing the existing security architecture and, conduct a security design audit and recommending improvements." 3. This Unit provides students training in what would be classified as "Compliance" in Cybersecurity	1. This Unit's focus is on compliance and not on Offensive, "Red Team" tactics. 2. This Unit does not require hands-on training in Offensive Cybersecurity or Penetration Testing.	This unit trains students in the policies and security architecture of an organization. It doesn't give practical training to test and secure infrastructure.

Offensive Cybersecurity

Proposed Course

Summary

Proposed Course Name: Offensive Cyber Security

Stated Learning Outcome:

The course focuses on hands-on training of Offensive Cyber Security Active Measures. Students get in-depth practical knowledge on various modules like - Network Security, Web Application Security, Mobile Application Security, Digital Forensics, Incident Response, Active Directory Pentesting, Windows Server 2016, Bypassing the perimeter, Privilege Escalation attacks. HackerU's proposed course provides in-depth and hands-on practical training in Offensive Cyber Security Active Measures. HackerU's Course is provides training in an environment that is as close to what is required in the cybersecurity industry as possible. Real-life simulations gives the student a place to apply the course's theoretical knowledge on the latest methods of penetrating the infrastructure. HackerU's course is kept current and prepares graduates for the international standard professional exam, the OSCP, as well as to prove competence to employers on a level suitable for a junior position on a "Red Team" in the cybersecurity industry immediately after graduation.

Post Comparison Analysis Summary:

The Offensive Cyber Security syllabus focuses mainly on giving hands-on experience to the learners which will help them to establish their position in the security industry. The syllabus gives them in-depth knowledge about the terminologies and concepts in Offensive Cyber Security Active Measures which makes the student fit to pass any hands-on and practical industry-standard cybersecurity certification such as the OSCP. The topics like Web Application Security, Mobile Application Security, and Infrastructure security prove competence to employers or potential clients in Offensive ""Red Team"" tactics.

The current courses accredited by ASQA, available in the National VET Registry, and are widely available to the public, focus heavily on compliance and some aspects of Defensive Cybersecurity. In conclusion, there is no possible combination of units currently registered with the National VET Registry, that can create a learning outcome similar to HackerU's proposed course: Class IV Certificate in Offensive Cybersecurity.

Sr. No	Unit Name	Learning Objectives	Remarks
1	Introduction to Cyber Security	1. This Unit gives theoretical knowledge about the basics of Networks and Networking. It discusses various tools and terminologies like Wireshark and OSI Layer in order to effectively learn the security fundamentals. 2. This Unit also discusses concepts like Cyber Attack Cycle, and various terminologies like Vulnerability, Exploit, Payload, etc in order to form the foundation of knowledge in Penetration Testing concepts. 3. The students will have hands-on experience regarding different attacks like network scanning and Brute Force 4. This Unit trains students in virtualization which includes Type 1 and Type 2 Hypervisors, as well as different types of Network modes. The subject of virtualization relates to Offensive Cybersecurity.	This unit acts like a building block for the learners and mainly prepares them for the advanced training of the course. This unit covers the basic understanding of networking, virtualization and cyber security concepts.
2	Linux Fundamentals	This Unit gives hands-on training of the Linux Operating system and trains students in properly configuring various services like FTP, SSH, Telnet, Apache, SQL in Linux.	This unit gives basic understanding of Linux Operating System and its fundamentals. Since linux is the most used OS in Cyber Security, it prepares the students to get familiar with Linux services and commands which will help the learners in advanced training.

Sr. No	Unit Name	Learning Objectives	Remarks
3	Windows Server 2016	1. Complete hands-on training in Setting Up Server-Client Architecture. 2. Focussing on Best security practices in an Administration Role. 3. Practical Assessment: Solving Real-time Challenges.	This module trains students to configure the Windows Server and Domain Controller. The Windows Server is the most used by organizations to create an environment. It is important to know secure configurations and common security threats while installing and creating a server-client model, all of which the student will prove full competence in actively and independently completing.
4	Bypassing The Perimeter	1. Hands-on training on OSINT, Recon, Enumeration, and getting into the environment using phishing attacks, Brute force. 2. Attacking using Metasploit which is one of the most well-known and used frameworks in the Security industry. 3. Detailed hands-on training on Wifi Hacking which helps in Offensive Cyber Security Active Measures assessment. 4. Practical Assessment: Solving Real-time Challenges.	This module trains students from a beginner level to an advanced level on methods of discovering, probing, and leveraging loopholes to test an organization's security. This module gives in-depth hands-on training on the most important and useful framework i.e Metasploit. Metasploit is used by most cybersecurity professionals on day to day basis.

Sr. No	Unit Name	Learning Objectives	Remarks
5	Cross Platform Elevation of Privileges	1. This Unit provides hands-on training on Escalating the privileges and conquering the entire environment with Admin rights. The student proves competence through real-time scenarios of Offensive Cyber Security Active Measures assessment. 2. This Unit provides hands-on training on most of the well-known attack methods which have been, and are currently being used. These methods have affected the entire world, Like - EternalBlue, Dirty cow, etc. 3. This Unit provides hands-on training in the escalation of privileges in Windows and Linux Environments which prepares students for Offensive Cyber Security Active Measures assessments, penetration testing jobs, and passing rigorous hands-on professional certifications. 4. Practical Assessment: Solving Real-time Challenges.	This Unit gives students hands-on training in ways to enhance the privileges of the owned system. The Unit trains students in methods used to successfully penetrate the security of a device or application, in order to get Administrator access to the application. By knowing the methods by which bad actors can beat defenses, organizations can develop custom security measures, policies, and technology, unique to their tech infrastructure to defend against loopholes in their system.
6	SIEM & SOC	1. This unit provides to the students hands-on training regarding security measues in an organization. 2. This unit will introduce the students with the state of mind of the defensive teams and will improve their attacking methodologies. 3. Hands-on training on end-point investigation which includes windows live & offline analysis and memory analysis. 4. The students will learn in this unit to investigate malwares and gathering information regarding the malicious file.	This module introduce with the students with Splunk SIEM, Pfsense Firewall, Snort IDS/IPS and provide them the full picture on the correlation between all the security measures. The second part of this module will be focused on the Digital Forensic and Incident Reponse. This module gives hands-on training on Windows investigation and suspicious file analysis.

Sr. No	Unit Name	Learning Objectives	Remarks
7	Advanced Infrastructure Attacks	1. This Unit focuses on the hands on training students to move around within an organisation from scratch i.e From one system to another. 2. This Unit covers tactics like getting into the environment by using unique exploitation techniques. 3. This unit can help a Red Team Operator understand and counter malicious actors from getting access from the entry level employee to a CEO. A requirement for the Offensive Cyber Security Active Measures assessment and the Industry Standard in Professional Certifications. 4. Practical Assessment: Solving Real-time Challenges.	This module gives hands-on training on Active Directory attacks. Various types of active directory attacks which are used mostly in Red team assessments to test the security of an organization.
8	Python for Hacking	1. Provides students with hands on practical training, taking them from no knowledge to advanced practical application in the Python coding language. 2. Includes hands-on training for students to create security tools themselves, and automate the day to day repetative tasks in cybersecurity. 3. Practical Assessment: Solving Real-time Challenges.	This Unit gives hands-on training in practical application of Python Scripting. The means which students can automate the security tasks and create security scripts for penetration testing of an organization's security. This unit also prepares learners to work in the company where it is needed to create scripts in order to automate the tasks and this will also help them to clear the screening round when joining the company for the job.
9	Web Fundamentals	1. This unit introduced students to the fundamentals of web development such as HTML, CSS, and Javascript. 2. This unit also prepares students to build web pages and small websites using web technologies. 3. This unit is base for the Web App Penetration testing module	This unit prepares students for the fundamentals of the web application. Before performing a security assessment on any web application, it's essential to know the fundamentals of how the web works, and this module exactly helps students in preparing small web applications and understand it's working.

Sr. No	Unit Name	Learning Objectives	Remarks
10	Web Application PT	1. This Unit provides students with hands-on training in finding from common basic to unique advanced vulnerabilities. 2. This Unit provides students with hands-on training in exploiting the vulnerabilities in a web application. 3. This Unit also focuses on basic web development through which students can understand the working of the web applications. 4. This Unit provides students with hands-on training in exploiting the most recent vulnerabilities. 5. This Unit provides students with hands-on experience using scanners and tools. 6. This Unit provides students with hands-on training on various open-source deliberately vulnerable applications. 7. Practical Assessment: Solving Real-time Challenges.	This Unit's objective is to train students to prove competence in one of the most in-demand skills of Cybersecurity. It gives hands-on training in Web Application Security and also provides training on various ways to leverage exploits and bugs found in the application.
11	Mobile Application PT	1. Focus on hands-on training of best security practices in mobile applications. 2. Hands-on training on Various tools used to exploit, check the vulnerabilities. 3. Hands-on training on various open-source deliberately vulnerable applications. Hands-on training on Exploiting most recent vulnerabilities. 4. Practical Assessment: Solving Real-time Challenges.	This Unit trains students using hands-on training to prove competence in the security of mobile applications. It gives hands-on training in finding vulnerabilities in Mobile Applications and leveraging those loopholes for owning the application.

Sr. No	Unit Name	Learning Objectives	Remarks
12	OSCP Preperation	1. Focus on hands-on training to the OSCP certification. 2. The students will learn the certification guildlines, introduce with previous exams and examples.	This unit trains the students to the OSCP exam to improve the state of mind and the methodlogies that will be used during the exam.

Topic	Certificate IV in Cyber Security	Advanced Diploma of Cyber Security	Proposed Course In Offensive Cyber Security Active Measures
Fundamentals of Network and Cyber Security.	**Yes**	**Yes**	**Yes**
Fundamentals of Virtualization and Cyber Infrastructure.	**Partially**	**Partially**	**Yes**
Cyber Attack Cycle	**No**	**No**	**Yes**
Linux Fundamentals	**No**	**No**	**Yes**
Windows Server, Domain, AD Setup	**Partially**	**Partially**	**Yes**
WireShark	**Yes**	**Yes**	**Yes**
OSINT & Recon	**Yes**	**Partially**	**Yes**
Brute Force & Password Cracking	**No**	**No**	**Yes**
Social Engineering and Phishing	**Yes**	**Partially**	**Yes**
Wifi Attacks	**Yes**	**Yes**	**Yes**
Metasploit Framework	**Yes**	**No**	**Yes**
Windows/Linux Privilege Escalation	**No**	**No**	**Yes**
Post Exploitation techniques	**No**	**No**	**Yes**
Tunneling & Pivoting	**No**	**No**	**Yes**
Active Directory Attacks	**No**	**No**	**Yes**
Obfuscation & AV Evasion	**No**	**No**	**Yes**
Lateral Movement	**No**	**No**	**Yes**
Powershell for Security	**No**	**No**	**Yes**
Python Fundamentals	**Yes**	**Yes**	**Yes**
Python for Offensive Security and Automation	**No**	**No**	**Yes**
Web Fundamentals	**No**	**No**	**Yes**
Web Application Penetration Testing	**Partially**	**Yesw**	**Yes**
Advanced Web Attacks	**No**	**No**	**Yes**
Mobile (Android) Security	**No**	**No**	**Yes**
Buffer Overflow Attack	**No**	**Yes**	**Yes**
SIEM	**Yes**	**Yes**	**Yes**
Security Measures	**Yes**	**Yes**	**Yes**
Windows Live & Offline Analysis	**No**	**No**	**Yes**
Memory Analysis	**No**	**No**	**Yes**
Basic Static Analysis	**No**	**No**	**Yes**
Basic Dynamic Analysis	**No**	**No**	**Yes**

Proposed Course Curriculum

Appendix C.

Proposed Course Curriculum

Module 1

Online Red Team Preparation Aptitude Assessment

Number of Instruction Hours

42.5

Total Hours Per Module (Academic)

57.5

Unit Number	Unit Title	Unit Topics
1	Introduction to Cyber	Cyber Security terms & attacks
2	Computer Hardware & OS	Computer hardware objects and operation systems
3	Virtualization Fundamentals	Virtualization Fundamentals
4	Introduction to Networking	Network fundamentals and component in corporate network
5	Networking Models & Segmentation	OSI/TCP IP Modles and IP & Subnetting
6	Linux Fundamentals	Basic Linux commands and usage
7	Cyber Attack Cycle	Cyber Attack Cycle steps and Brute Force attack in Linux
8	Exam + Cywar Challenges (Exam --> 1.5 hours)	Sorting Exam & Introductory Cywar Challenges

Module 2

Linux Fundamentals

Number of Instruction Hours

13

Total Hours Per Module (Academic)

20

Unit Number	Unit Title	Unit Topics
9	Introduction to Linux	Linux Fundamentals & Basic Commands (File System navigation, file creation)
10	Users, Groups & Permissions	Permission in Linux and Users types
11	Network Configuration & Package Management	Network Troubleshooting and configuartion, Installing packages
12	Configuring Services	Configuring Apache2,FTP,Samba,telnet
13	Final Project - Linux Fundamentals	

Module 3

Windows Server 2016

Number of Instruction Hours

13

Total Hours Per Module (Academic)

20

Unit Number	Unit Title	Unit Topics
14	Creating an Organization	Workgroup vs Domain Environments GUI vs Core Server Roles & Features
15	Active Directory Management	Server Roles & Features Creating a Forest
16	Working with Services (DHCP & DNS)	ConÞguring DNS & DHCP Managing Active Directories Creating Objects Creating Groups Installation of Additional Clients (Win7/10) Adding & Connecting Clients to the Domain
17	GPO Management	Group Permissions Access Control Group Policy Objects
18	Final Project - Windows Server	

Module 4

Bypassing the Perimeter

Number of Instruction Hours

26

Total Hours Per Module (Academic)

40

Unit Number	Unit Title	Unit Topics
19	WireShark	TrafÞc Analysis using WireShark Protocols Intercept Data Extraction
20	MITM	Man In the Middle Attack Arpspoof dnspoof
21	OSINT & Social Engineering	Social Engineering Phishing Site Cloning SEToolkit
22	Network Scanning	Detetcing online hosts Hping3 Nmap Banner Brabber

Unit Number	Unit Title	Unit Topics
23	Password Cracking	Brute Force Dictionary Attack cupp Crunch
24	MetaSploit &Known CVEs	Creating Payloads Command & Control Bind Shell/Reverse Shell Metasploitable Training
25	Wi-Fi Attacks	Wi-Fi Cracking Airmon-ng aireplay-ng aircrack wifite
26	Web Anonymity	Darknet TOR Onion Layers Proxychains
27	Final Project - Bypassing the Perimeter	

Module 5

Cross Platform Elevation of Privileges

Number of Instruction Hours

19.5

Total Hours Per Module (Academic)

30

Unit Number	Unit Title	Unit Topics
28	Windows Local Privilege Escalation	Windows Permissions Windows Privilege Escalation Ease of access manipulation Users Creation
29	Windows Post Exploitation & Credentials Dumping	Credenitals Dumping Mimikatz Windows OS Vulneble protocols & files Covering tracks
30	Linux Local PE & Post Exploitation	Grub Bypassing Sudo privilege File system mounting
31	Linux Automated Tasks & Permission Misconfiguration	Post Exploitation Techniques Credential Extraction Persistence & Hidden Users Covering the Tracks

Unit Number	Unit Title	Unit Topics
32	Common Exploits & Buffer Overflow	Dirtycow Eternalblue Bluekeep
33	Unquoted Services & DLL Hijacking	Unquoted Service DLL Hijacking DLL Injection Procmon msfvenom
34	Final Project - Cross Platform Elevation of Privileges	

Module 6

SIEM & SOC

Number of Instruction Hours

32.5

Total Hours Per Module (Academic)

50

Unit Number	Unit Title	Unit Topics
35	SIEM & SOC Introduction	SOC Roles SOC Structure SOC Work Flow Enterprises Architectures TMS
36	End-Point Protection	Anti-Virus End-Point Solutions EDR DLP ESET ESMC ESMC Group & Tasks

Unit Number	Unit Title	Unit Topics
37	Network Protection & Prevention	Firewall WAF IDs/IPS NAC Pfsense
38	Log Generation & Collection	Logs Structure Event Viewer Syslog
39	SIEM Solutions	SIEM Splunk
40	IOC & Malwares	IOC Malware Magic Numbers
41	Windows Live & Offline Analysis	Live Forensics Process Investigation DNS Cache Digital Forensics & Incident Response
42	Memory Analysis	Memory Dump Memory Investigation Volatility
43	Basic Static Analysis	Strings SigCheck Virus Total HxD Magic Bytes

Unit Number	Unit Title	Unit Topics
44	Basic Dynamic Analysis	Dependency Walker Regshot Sysmon Autoruns
45	Final Project - SIEM & SOC	

Module 7

Advanced Infrastructure

Number of Instruction Hours

32.5

Total Hours Per Module (Academic)

50

Unit Number	Unit Title	Unit Topics
46	Enumerating an Organization	RSAT Bloodhound Sharphound Neo4j
47	Lateral Movement	WMI WinRM PsExec Pass the Hash
48	SMB Relay & Responder	LLMNR Manipulation Responder SMB Relay Inveigh

Unit Number	Unit Title	Unit Topics
49	PowerShell as a Weapon	Powershell Basics Powershell Policies Scripts creation Exploitation via PowerShell
50	Obfuscation Techniques	Manual Obfuscation Invoke-Obfuscation Obfuscation Frameworks
51	Office Exploitation	VBA Macro Formula Injection SFX
52	Exploiting Services within an organization	Mail Relay Heartbleed Redis SSH Keys Manipulation
53	Reverse Shells & Tunneling	Bind Shell & Reverse Shell ICMP Tunneling SSH Tunneling DNS Tunneling Dnscat2
54	Kerberoasting & Pass the Ticket & Module Review	Pass the ticket Golden Ticket Invoke-Kerberoasting
55	Final Project - Advanced Infrastructure	

Module 8

Python for Ethical Hacking

Number of Instruction Hours

26

Total Hours Per Module (Academic)

40

Unit Number	Unit Title	Unit Topics
56	Introduction to Python	PyCharm Variables Types Casting Conditions Mathematical Operators
57	Data Types & Loops	Data Structure For Loop While Loop Tuple Dictionary List
58	Functions & Code Handling	Function Creation Dateime Psuedo Random

Unit Number	Unit Title	Unit Topics
59	File System & Error Handling	Try & Except Exception Types File Permissions OS Module Log Parsing
60	Web Communication	Urllib3 Requests BeautifuSoup
61	Sockets Fundamentals	Client-Side Socket Server-Side Socket Data Exchange Echo Communication
62	Protocols Communication	Banner Grabber Protocol Investigation FTP Breakdown
63	Scapy & Network Scanning	Scapy Fundamentals Sending & Receiving Packets Port Scanner ARP Scanner ARP Spoofer
64	Final Project - Python for Hacking	

Module 9

Web Fundamentals

Number of Instruction Hours

19.5

Total Hours Per Module (Academic)

30

Unit Number	Unit Title	Unit Topics
65	Introduction to HTML	Internet Technologies HTML Fundamentals Structuring Web Pages
66	CSS Fundamentals	CSS Design The Box Model CSS for Hackers
67	JavaScript Fundamentals	Arithmetical Operations Document Object Model JavaScript for Hackers
68	Building Web Pages	Web Application Structure Use Input & Forms XAMPP Web Server Using PHP in XAMPP

Unit Number	Unit Title	Unit Topics
69	Advanced JavaScript	Functions Array & Loops Debugging JavaScript Obfuscation
70	Introduction to Server-Side	XAMPP Installation PHP Implementation PHP Data Types PHP Programming
71	Final Project - Web Fundamentls	

Module 10

Web Application Penetration Testing

Number of Instruction Hours
39

Total Hours Per Module (Academic)
60

Unit Number	Unit Title	Unit Topics
72	Web Technologies	RSAT Bloodhound Sharphound Neo4j
73	PHP Vulnreabilities & OWASP Top 10	PHP Configuration Secure Coding OWASP TOP 10 Web PT Prerequisites
74	Burp & ZAP	Burp Suite Setup Burp Suite Components ZAP

Unit Number	Unit Title	Unit Topics
75	XSS	DOM XSS Reflected XSS Persistence/Stored XSS Security Measures Evasion
76	Database Management	Relational Database MySQL SQL Syntax
77	SQL Injection	Attacking Vectors SQL Injectgion Execution Boolean Based Bypass Authentication
78	Advanced SQL Injection	Blind SQLi SQLmap Bypassing Security Measures Website Enumeration
79	NoSQL Injection	MongoDB NoSQL Injection
80	CSRF & Broken Authentication	Authorization Broken Authentication CSRF

Unit Number	Unit Title	Unit Topics
81	XXE & SSRF	SSRF Execution XML External Entities Exploitation with XML Entities
82	LFI/RFI to RCE & WordPress Hacking	Local File Inclusion Remote File Inclusion File Upload Bypass WordPress Hacking WPScan
83	PT Flow & Reporting and Vulnerabilities Scanning	Penetration Testing Types Penetration Testing Toolkit Penetration Testing Report Vulnerability Scanners Website Scanners
84	Final Project - Web Application Penetration Testing	

Module 11

Mobile Security

Number of Instruction Hours
26

Total Hours Per Module (Academic)
40

Unit Number	Unit Title	Unit Topics
85	Introduction to Android	Android Files System Dalvik vs ART Apk Structure Dex2Jar JD-GUI
86	Android Programming	Android Activities Android Studio Programming Java Functions
87	Android Reversing	APK Reversing Smali Code ApkTool Jadex APK Sign

Unit Number	Unit Title	Unit Topics
88	Android Traffic Analysis	Traffic Interception Burp Suite Frida
89	SSL Pinning	SSL Verification SSL Pinning ByPass FRIDA Scripts
90	Android Malwares & Run Time Debugging	Msfvenom Meterpreter Android Payload Execution APK Debugging
91	Static & Dynamic Investigation Frameworks	MobSF Drozer
92	iOS Security	Jailbreak iMazing appinst Clutch
93	Final Project - Mobile	

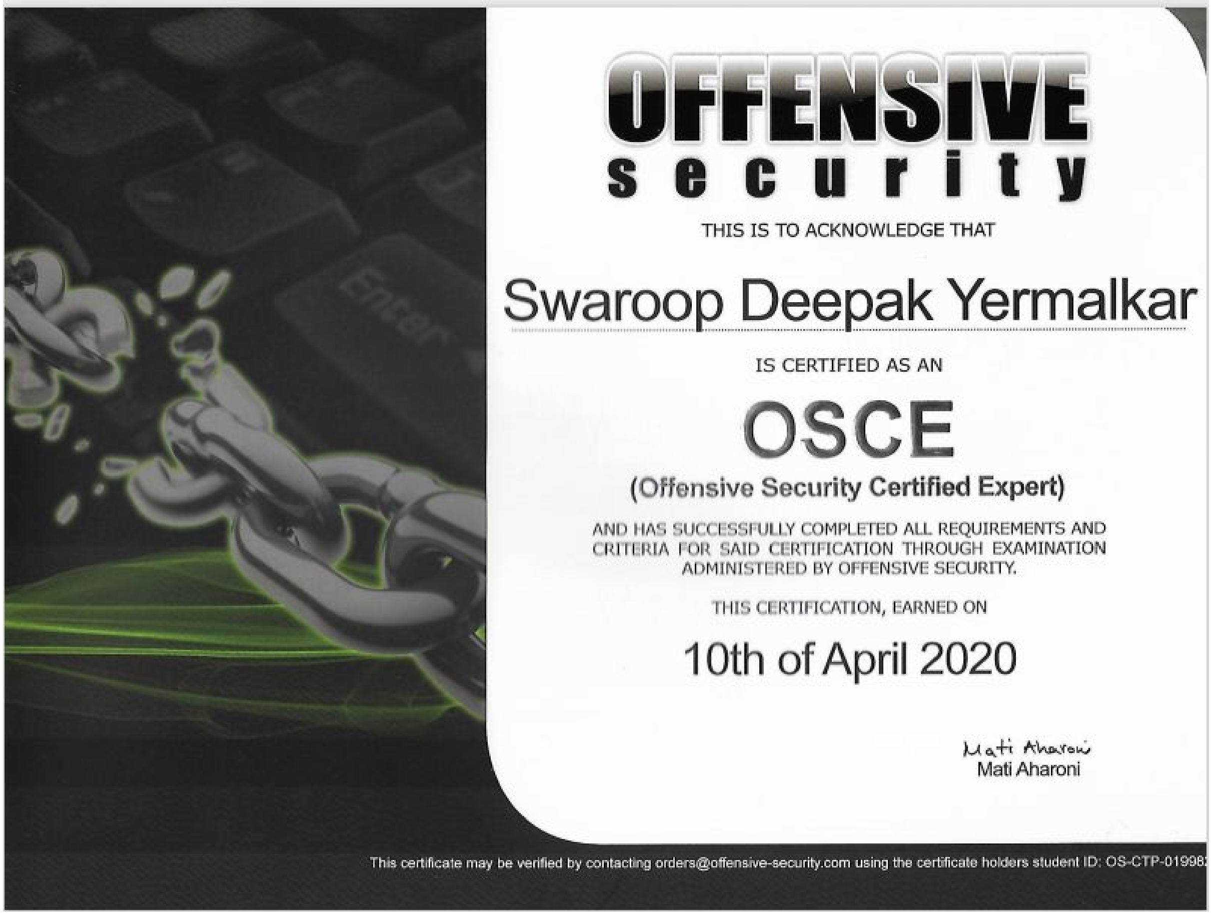
Module 12
OSCP Preperation
Number of Instruction Hours 32.5
Total Hours Per Module (Academic) 50

Module 13
Career Services
Number of Instruction Hours 8.5
Total Hours Per Module (Academic) 12.5

Hours Breakdown	Total Hours
Total Course Hours without Final Projects (Clock)	400
Toatal Course hours without Final Projects (Academic)	500
Total Final Projects (Clock)	100
Total Final Projects (Academic)	125
Total time without break (Clock without Final Projects)	330.5
Total time without break (Academic without Final Projects)	413.1
Total Course Hours + Final Projects(Clock)	500
Total Course Hours + Final Projects(Academic)	625

Appendix D.

Credentials Of Technical Audit Lead



OFFENSIVE security

THIS IS TO ACKNOWLEDGE THAT

Swaroop Deepak Yermalkar

IS CERTIFIED AS AN

OSCE

(Offensive Security Certified Expert)

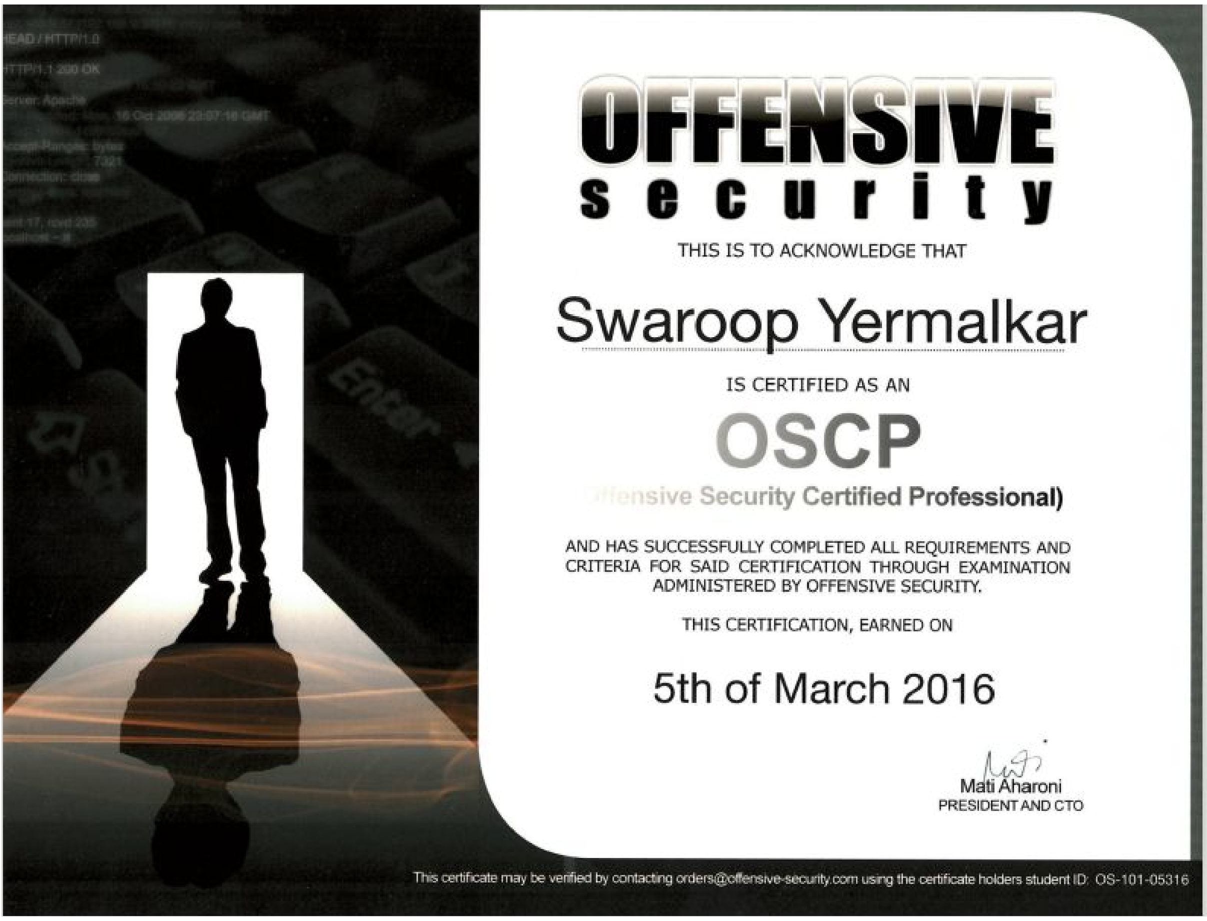
AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.

THIS CERTIFICATION, EARNED ON

10th of April 2020

Mati Aharoni
Mati Aharoni

This certificate may be verified by contacting orders@offensive-security.com using the certificate holders student ID: OS-CTP-01998



HEAD / HTTP/1.0
HTTP/1.1 200 OK
Server: Apache
Accept-Ranges: bytes
Connection: close
Enter
Shift

OFFENSIVE security

THIS IS TO ACKNOWLEDGE THAT

Swaroop Yermalkar

IS CERTIFIED AS AN

OSCP

(Offensive Security Certified Professional)

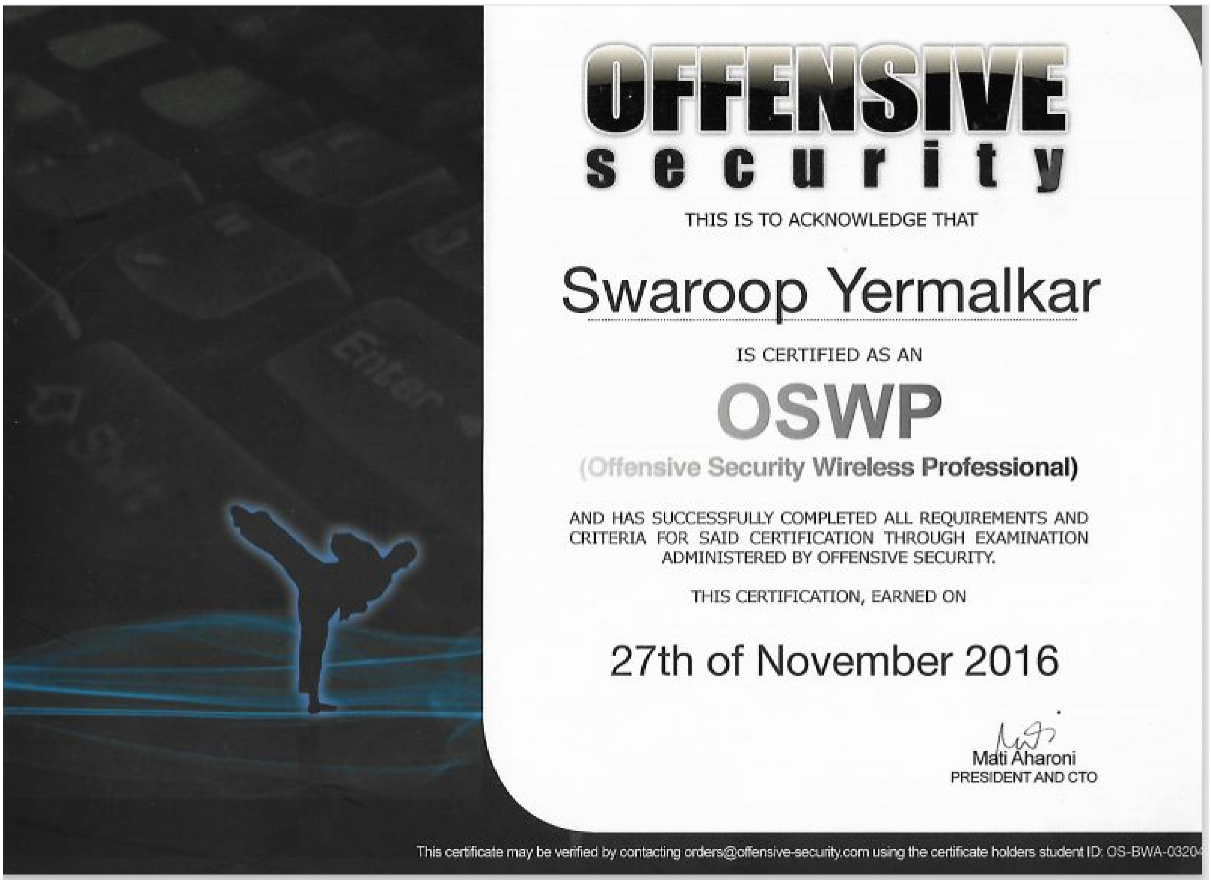
AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.

THIS CERTIFICATION, EARNED ON

5th of March 2016

Mati Aharoni
PRESIDENT AND CTO

This certificate may be verified by contacting orders@offensive-security.com using the certificate holders student ID: OS-101-05316



Enter
Shift

OFFENSIVE security

THIS IS TO ACKNOWLEDGE THAT

Swaroop Yermalkar

IS CERTIFIED AS AN

OSWP

(Offensive Security Wireless Professional)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.

THIS CERTIFICATION, EARNED ON

27th of November 2016

Mati Aharoni
PRESIDENT AND CTO

This certificate may be verified by contacting orders@offensive-security.com using the certificate holders student ID: OS-BWA-03204

#WHOAMI

Swaroop Yermalkar

- Head of Cyber Security - Red Team for HackerU India
- 8+ years of industry experience! Worked with Philips Healthcare, Lithium, Traveloka, Persistent in the past.
- Holds OSCE, OSCP, OSWP, CREST Certified
- Speaker at AppSec USA 2018, Defcon 27 (AppSec Village), AppSec Israel, AppSec USA 2017, BruCON, SEC-T, HITCON (Taiwan), Bugcrowd Level Up, GroundZero, c0c0n, EuropeanSec
- Synack Rank #1 (worldwide) Mobile Bug Bounty Hunter, One of top pentester at Cobalt
- **OWASP iGoat Project Lead** (https://igoatapp.com/)
- Acknowledged by Microsoft, Amazon, Etsy, Dropbox, Evernote, Simple banking for reporting high severity security issues

Authored Books

Learning iOS Penetration Testing

by Swaroop Yermalkar | 7 January 2016

★★★★☆ 17

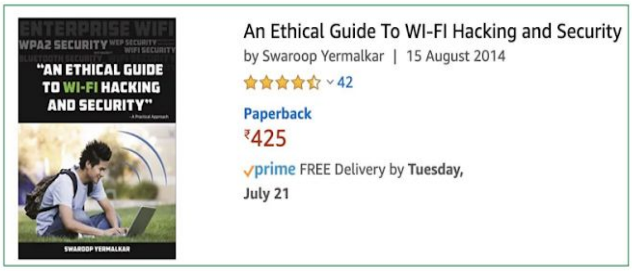
Kindle Edition

₹669^{89}

Paperback

₹1,987 ~~₹2,799~~ Save ₹812 (29%)

✓prime FREE Delivery by **Friday, July 24**



An Ethical Guide To WI-FI Hacking and Security

by Swaroop Yermalkar | 15 August 2014

★★★★☆ 42

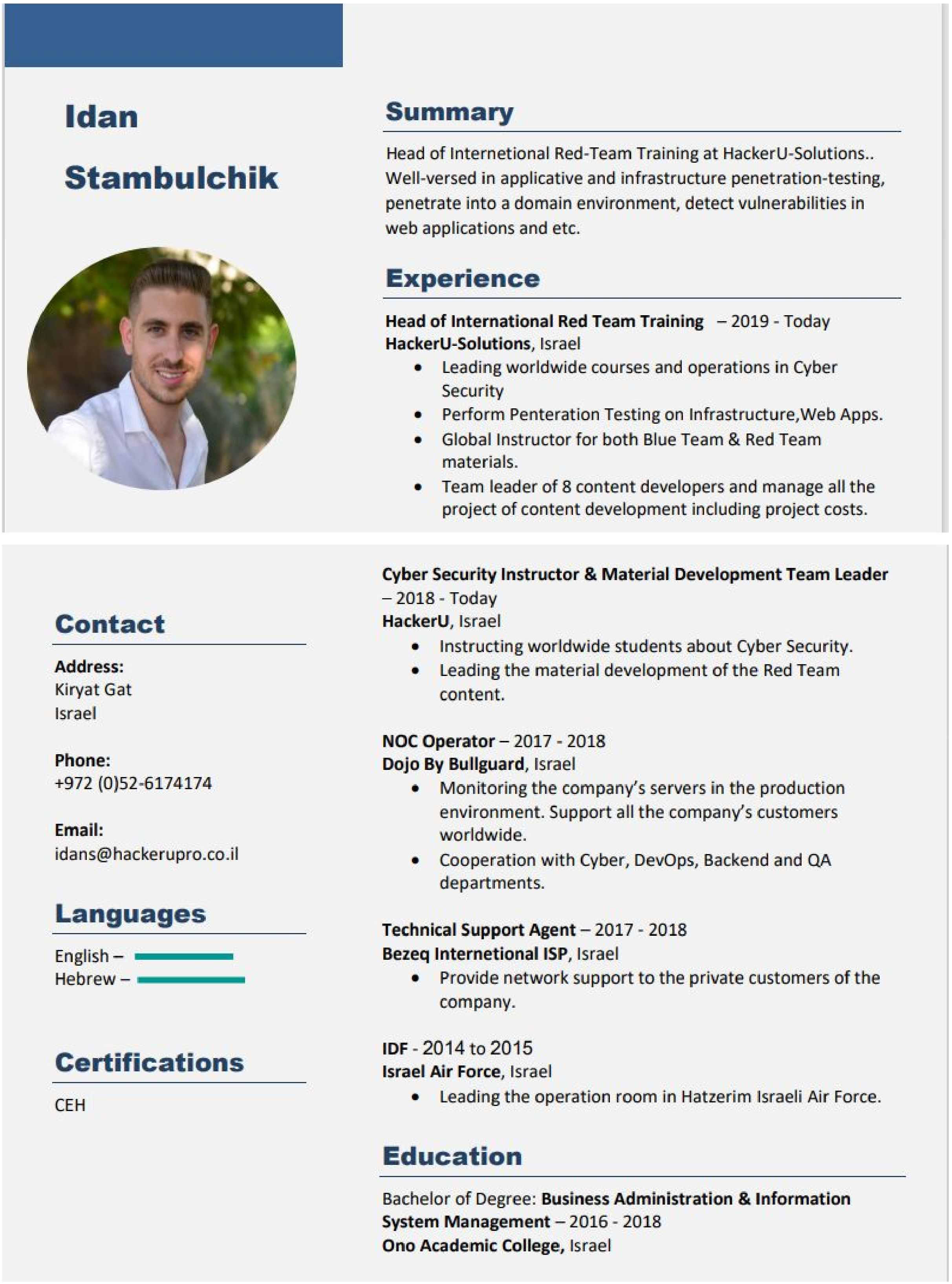
Paperback

₹425

✓prime FREE Delivery by **Tuesday, July 21**

Appendix E.

Credentials Of Technical Audit Review



Idan Stambulchik

Summary

Head of Internetional Red-Team Training at HackerU-Solutions.. Well-versed in applicative and infrastructure penetration-testing, penetrate into a domain environment, detect vulnerabilities in web applications and etc.

Experience

Head of International Red Team Training – 2019 - Today
HackerU-Solutions, Israel

- Leading worldwide courses and operations in Cyber Security
- Perform Penteration Testing on Infrastructure,Web Apps.
- Global Instructor for both Blue Team & Red Team materials.
- Team leader of 8 content developers and manage all the project of content development including project costs.

Cyber Security Instructor & Material Development Team Leader – 2018 - Today
HackerU, Israel

- Instructing worldwide students about Cyber Security.
- Leading the material development of the Red Team content.

NOC Operator – 2017 - 2018
Dojo By Bullguard, Israel

- Monitoring the company's servers in the production environment. Support all the company's customers worldwide.
- Cooperation with Cyber, DevOps, Backend and QA departments.

Technical Support Agent – 2017 - 2018
Bezeq Internetional ISP, Israel

- Provide network support to the private customers of the company.

IDF - 2014 to 2015
Israel Air Force, Israel

- Leading the operation room in Hatzerim Israeli Air Force.

Education

Bachelor of Degree: **Business Administration & Information System Management** – 2016 - 2018
Ono Academic College, Israel

Contact

Address:
Kiryat Gat
Israel

Phone:
+972 (0)52-6174174

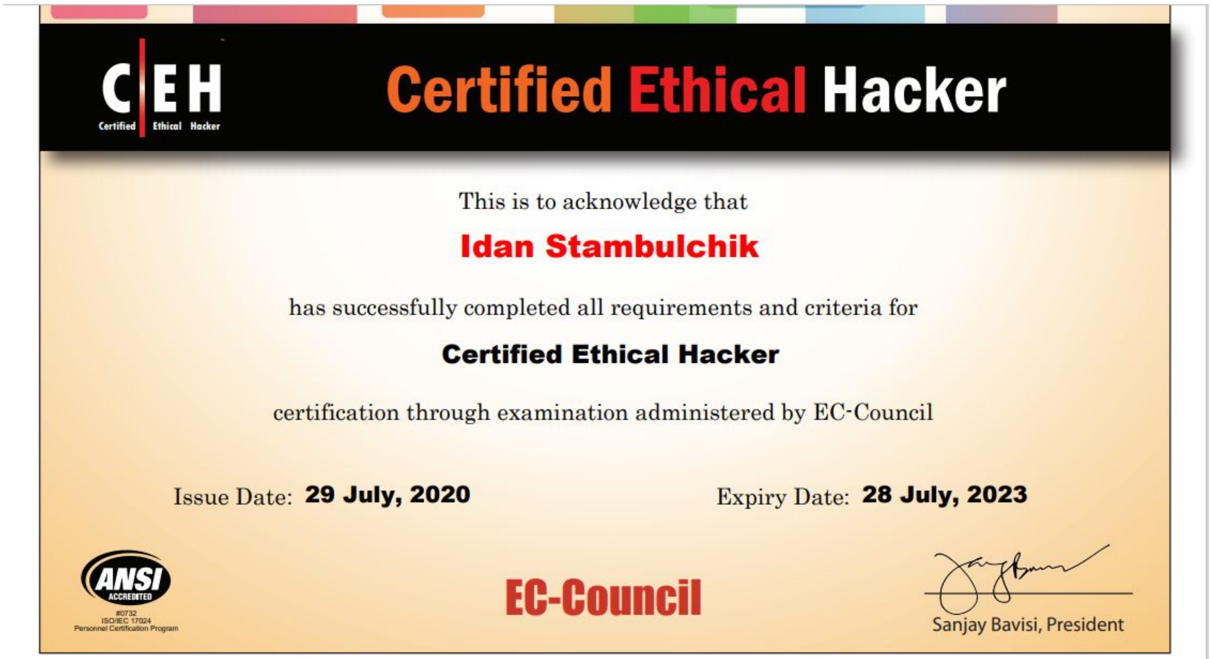
Email:
idans@hackerupro.co.il

Languages

English – ▬▬▬
Hebrew – ▬▬▬

Certifications

CEH



C|EH Certified Ethical Hacker

Certified Ethical Hacker

This is to acknowledge that

Idan Stambulchik

has successfully completed all requirements and criteria for

Certified Ethical Hacker

certification through examination administered by EC-Council

Issue Date: **29 July, 2020**

Expiry Date: **28 July, 2023**

ANSI ACCREDITED
#0732
ISO/IEC 17024
Personnel Certification Program

EC-Council

Sanjay Bavisi, President

Leaving No One Behind

The Digital Age

Student Enrollment Forecast

Student Enrollment Forecast

CONTRIBUTORS

Authored By:

Jesse Miller

Head Of International Development
& Government Relations

HackerU Global Education

Jessem@hackeru.com
+972.50.222.4978

Table Of Contents

Proposed Course - Uniqueness In the Market

1. As demonstrated in Section 2 of the Petition, there is no course or combination of existing units of competency which will achieve the same or similar learning outcomes of HackerU's proposed course.

2. There is a massive demand for highly specialized cybersecurity professionals. Unlike current courses on the market, the proposed course takes on specialized subject matter that is essential for any cybersecurity company but is only taught in very few Australian higher education institutions, and mostly in part, not as a full qualification.

3. The Uniqueness of the course's subject matter in the Australian education system, combined with the high market demand for qualified professionals, creates a unique opportunity for RTOs, TAFEs, and HackerU to partner together to train students in one of the fastest-growing industries in the tech sector, and potentially creating an economic impact country-wide.

4. The proposed course is designed to be a low-risk high reward scenario, accessible to everyone. The proposed course's design, like all of HackerU's courses, is made to create a pro-social movement in high tech knowledge transfer, removing barriers and discovering potential, growing the skills deficit with workers from all backgrounds.

Prospective Students

Motivation, Diversity, & Pro-Social Outcomes

1. Students who take part in HackerU's programs are from diverse backgrounds. Women, Minorities, Older Aged, and those from a lower socio-economic demographic are largely represented in contrast to a traditional IT cohort.

2. The design of the proposed program allows prospective students the opportunity to explore their aptitude as well as for the instructor to qualify candidates based on live coursework - specially designed to assess the probability of a student's success with the larger program.

3. The proposed program's curriculum and learning materials are designed to take a student with no prior experience or knowledge in IT, computer science, or cybersecurity, and bring them to a level where they are qualified for immediate employment in the cybersecurity industry in a specialized entry-level position.

4. Because the proposed program has these features, it requires no prerequisites. The assessment phase is typically free of charge for the student, which allows candidates who never might have considered this career path a risk-free way to explore the subject matter as a potential vocation, and as an educational pathway.

5. Because the cybersecurity industry worldwide suffers from a dramatic skill shortage, HackerU has worked to staff graduates. It has close to a 90% success rate in doing so and offers a job guarantee where the practice is legal.

6. Because of the applied, practical, and hands-on nature of the program, high demand for qualified professionals, and the ease of employment for graduates, prospective students view the program as low risk relative to the investment in their education.

7. Because of the accelerated learning structure, low cost relative to a degree program, and arguably higher financial benefits with employment, students who do not have the privilege required for a full degree program, such as a difficult economic situation, a lack of family support. Those who are older or responsible for a family, or are part of an industry that is declining or becoming obsolete, may find HackerU's program structure a workable solution to achieve social mobility.

8. For all previously stated reasons, HackerU, and the proposed course, attracts a diverse cohort, and a much broader audience than academic and theory-based programs that are part of University Degree programs.

9. The inclusive program design has pro-social consequences, as well as serious economic benefits. As outlined AustCyber in its 2019 Strategy Report, a key impediment in bringing investment, gaining a local presence of international cybersecurity conglomerates, and growing cybersecurity startups is a severe shortage of qualified and skilled manpower.

10. The course's design is for a broad audience and the low barriers to entry have resulted in large public awareness and, in turn, large student enrollment. This, combined with the practical knowledge and proven competence of graduates has allowed HackerU to graduate approximately 7000 students per year in Israel, many more in the US and Internationally, and has contributed for 20 years to Israel's position as a world leader in cybersecurity.

Why The American Proof Of Concept Is Relevant To Australia

1. HackerU entered the U.S. market much as it is entering the Australian market. Cybersecurity was widely known as a niche specialization for which only IT professionals were trained, and only in a university setting. While there always were alternative programs and accelerated learning boot camps, the quality was in question by both prospective students and employers.

2. Through aggressive marketing, mainly Pay Per Click advertising targeting an audience that is unemployed, underemployed, undereducated, underpaid, or part of an increasingly obsolete industry, HackerU has had major success in raising awareness of fast and efficient cybersecurity training. Serving both the public and industry by closing the skills gap with a diverse cohort of individuals who may not have the privilege or resources to pursue a 4-year degree.

3. The Australian market is remarkably similar to that of the United States in all metrics relevant to HackerU's pursuit. Demographic, Economic, and Socio-Economic data deviate little, as demonstrated in Appendix A.

4. Due to the similarities in all relevant data points between the two countries, we believe that any organization willing to take on similar methods of marketing will have a similar outcome in student enrollment.

Projection Methodology Summary

1. The Student Projection Methodology first compares the similarities of the United States and Australia in publicly available data. The comparison table can be found in Appendix A.

2. The focus is on Demographic and Economic Data, as well as other metrics relevant to the choices a prospective student may be weighed when someone is deciding whether or not to engage with a new course.

3. Because there is a remarkable similarity between countries in all relevant data points, averages are taken from HackerU's marketing and sales performance and are reliable variables to use in establishing awareness with the public, successful messaging, and successful enrollment.

4. The Metrics taken from marketing and sales are companywide and representative of the values in the US. A list of these variables can be found in Appendix E.

5. The model then uses mock campaigns in marketing channels that account for most of HackerU's advertising worldwide. These are Facebook Ads, and Google Ads respectively. The parameters of the mock campaigns were laid out as follows:

    a. The Duration of the Mock Campaign is 1 month simply as a unit that can be easily extrapolated

    b. The Total Budget represents HackerU's minimum commitment when entering a new market.

    c. The Budget Ratio is created according to averages taken company-wide, representative of the U.S.'s Facebook Ads to Google Ads ratio.

    d. Keywords are reflective of what is common in US campaigns.

    e. Location is based on Demographic data, Given that the Urban Density in Australia is 86.20%, the top 8 most populated cities were used.

    f. Audience / Demographics are based on median age and GDP per capita in Australia.

    g. All other information used to create the target audience, such as "interests" is based on the common practice in the US.

    h. The mock campaigns will establish:

        i. Reach
        ii. Impressions

    i. The Mock Campaign results can be viewed in Appendix B., C., and D.

6. Using the results from the 3rd party advertising platforms, we will apply the historic variables, factoring in sales cycle length, and create a date for our first cohort and number of students. These calculations can be reviewed in Appendix F.

7. We will extrapolate those results over 3 years (36 Months) to gather our student projections. These calculations can be reviewed in Appendix G.

Methodology

1. HackerU's Approved Budget For Awareness Campaign

2. Facebook Ads to Adwords Ratio In The U.S.

3. Estimates From Google Ads (Keyword Planner) Using Ratioed Budget & Relevant Keywords
    a. Reach
    b. Impressions
    c. Estimated CPC

4. Estimates From Facebook Ads Using Ratioed Budget, Relevant Keywords, & Audience
    a. Reach
    b. Impressions
    c. Estimated CPC (Using Historical Data As Key Variable)

5. Existing Marketing & Sales Data
    a. Average CTR
    b. Average Landing Page CR
    c. SQL to Stage1 (Free Sorting) Conversion Rate
    d. Stage1 Customer to Paid Student Conversion Rate
    e. Current average sales cycle length

6. Using Base Data From Google Ads & Facebook With Existing Variables To Extrapolate Projections Such As:
    a. CPC
    b. CPL
    c. CPA

7. Holding all else equal, the final Cost per Acquisition against:
    a. Budget
    b. Sales Cycle Length
    c. Minimum / Maximum Class Size

8. Using All Existing Known Data & Variables Establishing Final Projection:
    a. Projected New Cohort Frequency
    b. Projected Students Per Year
    c. Projected Students Over 3 Years *36 Months

Projection Conclusion

1. Based on the calculations laid out in the methodology, there can be a new course every 3 months, per institution with a maximum cohort size of 50 students.

2. After Q1 of running sales and marketing campaigns, the institution can expect 1 cohort with 40 students.

3. After 1 year *12 months the institution can expect 10 cohorts with 400 students

4. After 3 years *36 months, the institution can expect 32 cohorts, a total of 1,280 students enrolled, and the number of students enrolled monthly to hold steady

5. **Based on the conclusions outlined above, there will be more than enough potential students to justify the course's national recognition and accreditation by ASQA**

Appendix

Appendix A.

Data-Based Similarities To The U.S., Meaningful To Education Decisions

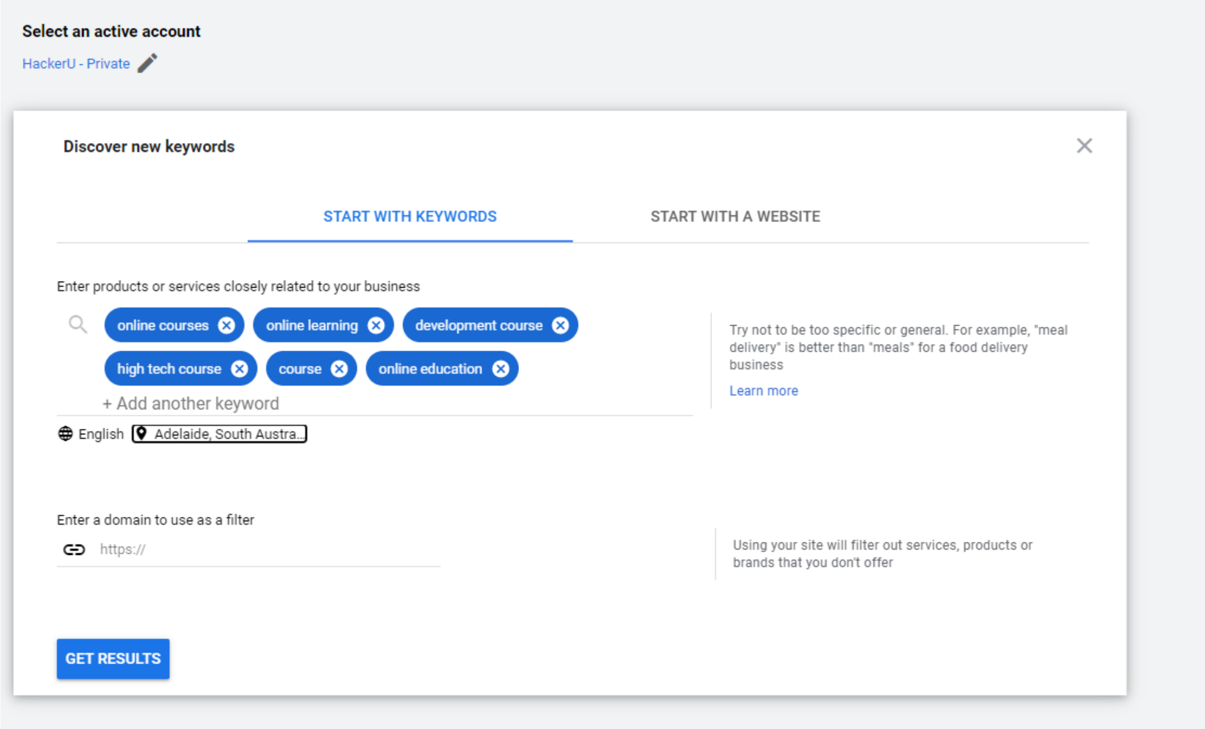
For all Data And Calculations Please See Spreadsheet

Relevant Metric	U.S.	Australia	Difference	Notes
Target Age Group (Population) 25-54 years:	38.92%	41.15%	**2.23%**	
Median Age	38.5	37.5	**-1**	
Urban Population % of total population (2020):	82.70%	86.20%	**3.50%**	
Dependency ratios total dependency ratio:	53.9	55.1	**1.2**	
youth dependency ratio:	28.3	29.9	**1.6**	
elderly dependency ratio:	25.6	25.1	**-0.5**	
potential support ratio: (2020 est.)	3.9	4	**0.1**	
GDP - per capita (PPP) (2017 est.)	$59,800.00	$50,400.00	**-$9,400.00**	data are in 2017 dollars
GDP - per capita (PPP) (2016 est.)	$58,900.00	$50,100.00	**-$8,800.00**	data are in 2017 dollars
GDP - per capita (PPP) (2015 est.)	$58,400.00	$49,600.00	**-$8,800.00**	data are in 2017 dollars
GDP - composition by sector (agriculture) (2017 est.):	0.90%	3.60%	**2.70%**	
GDP - composition by sector (industry) (2017 est.):	19.10%	25.30%	**6.20%**	
GDP - composition by sector (services) (2017 est.):	80%	71.20%	**-8.80%**	
Household income or consumption by percentage share lowest	10%: 2%	10%: 2%		
Household income or consumption by percentage share highest (2007 est.) / (1994)	10%: 30%	10%: 25.4%		
Inflation rate (consumer prices) (2017 est.)	2.10%	2%	**0%**	
Inflation rate (consumer prices) (2016 est.)	1.30%	1.30%	**0.00%**	

Internet users percent of the population (July 2018 est.):	87.27%	86.55%	**-0.72%**	
Broadband - fixed subscriptions per 100 inhabitants:	34	31	**-3**	
Education expenditures % of GDP (2014) / (2016)	5%	5.30%	**0.30%**	
Source	https://www.indexmundi.com/factbook/compare/united-states.australia			

Appendix B.

Forecasts From Advertising Platforms (Google Ads)



Select an active account

HackerU - Private

Discover new keywords

Enter products or services closely related to your business

online courses ⊗ online learning ⊗ development course ⊗ high tech course ⊗ course ⊗ online education ⊗

+ Add another keyword

English | Adelaide, South Austra...

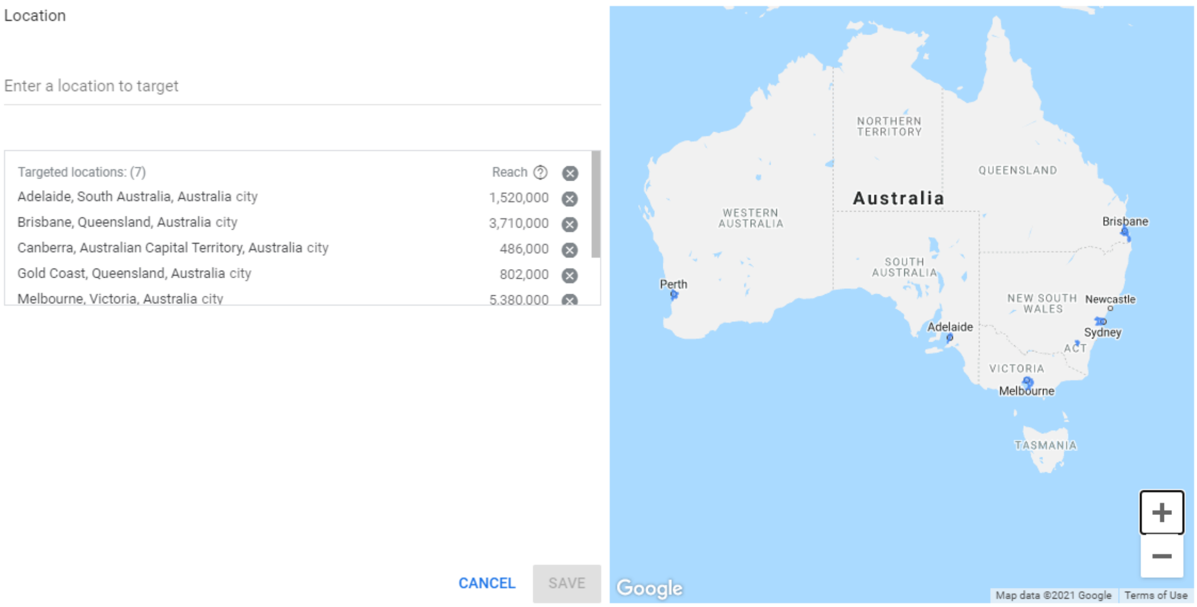
Try not to be too specific or general. For example, "meal delivery" is better than "meals" for a food delivery business

Learn more

Enter a domain to use as a filter

https://

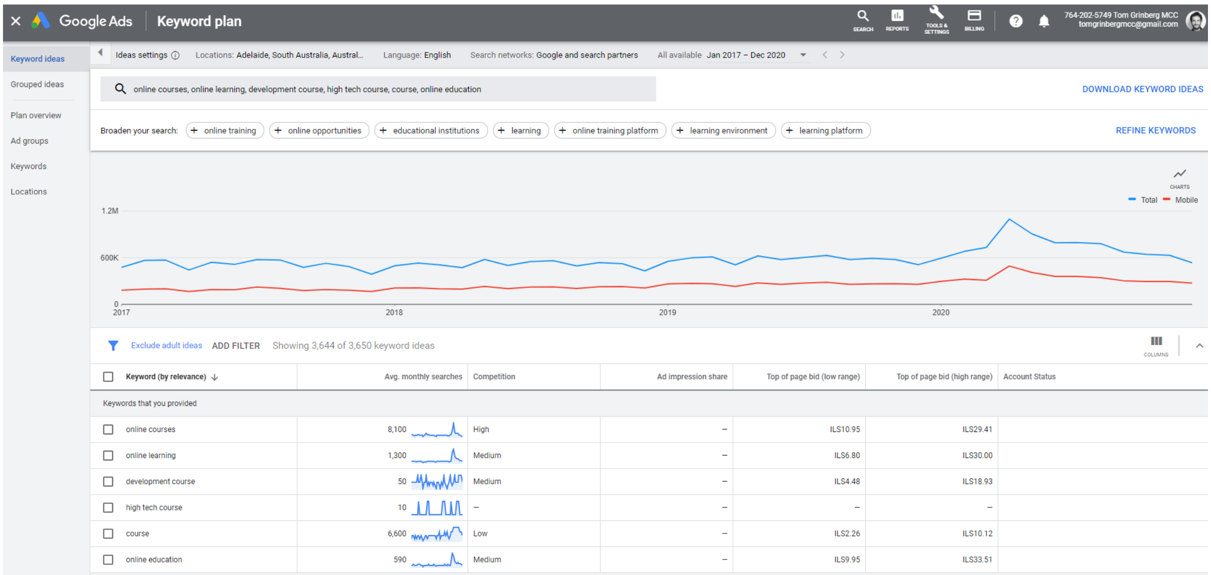
Using your site will filter out services, products or brands that you don't offer



Location

Enter a location to target

Targeted locations: (7)	Reach ⓘ	⊗
Adelaide, South Australia, Australia city	1,520,000	⊗
Brisbane, Queensland, Australia city	3,710,000	⊗
Canberra, Australian Capital Territory, Australia city	486,000	⊗
Gold Coast, Queensland, Australia city	802,000	⊗
Melbourne, Victoria, Australia city	5,380,000	⊗



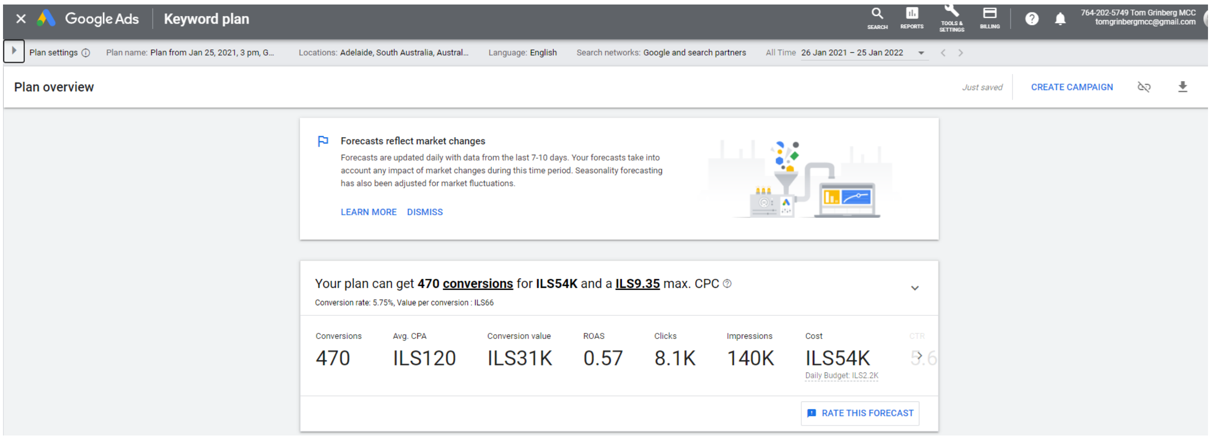
Ideas settings ⓘ Locations: Adelaide, South Australia, Austral... Language: English Search networks: Google and search partners All available Jan 2017 – Dec 2020

online courses, online learning, development course, high tech course, course, online education

Broaden your search: + online training + online opportunities + educational institutions + learning + online training platform + learning environment + learning platform

Exclude adult ideas ADD FILTER Showing 3,644 of 3,650 keyword ideas

□ Keyword (by relevance) ↓	Avg. monthly searches	Competition	Ad impression share	Top of page bid (low range)	Top of page bid (high range)	Account Status
Keywords that you provided						
□ online courses	8,100	High	–	ILS10.95	ILS29.41	
□ online learning	1,300	Medium	–	ILS6.80	ILS30.00	
□ development course	50	Medium	–	ILS4.48	ILS18.93	
□ high tech course	10	–	–	–	–	
□ course	6,600	Low	–	ILS2.26	ILS10.12	
□ online education	590	Medium	–	ILS9.95	ILS33.51	



Plan settings ⓘ Plan name: Plan from Jan 25, 2021, 3 pm, G... Locations: Adelaide, South Australia, Austral... Language: English Search networks: Google and search partners All Time 26 Jan 2021 – 25 Jan 2022

Plan overview

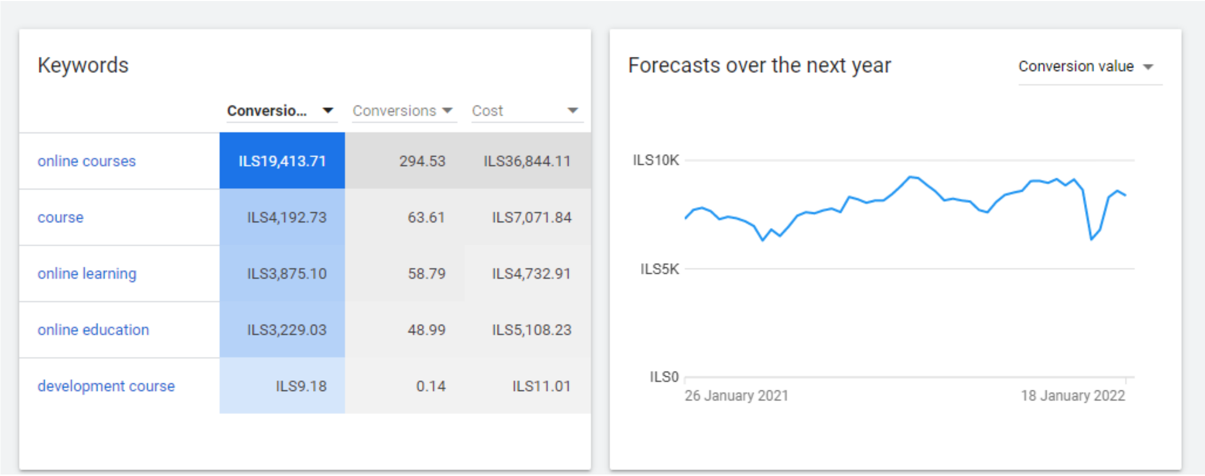
Forecasts reflect market changes

Forecasts are updated daily with data from the last 7-10 days. Your forecasts take into account any impact of market changes during this time period. Seasonality forecasting has also been adjusted for market fluctuations.

Your plan can get **470 conversions** for **ILS54K** and a **ILS9.35** max. CPC

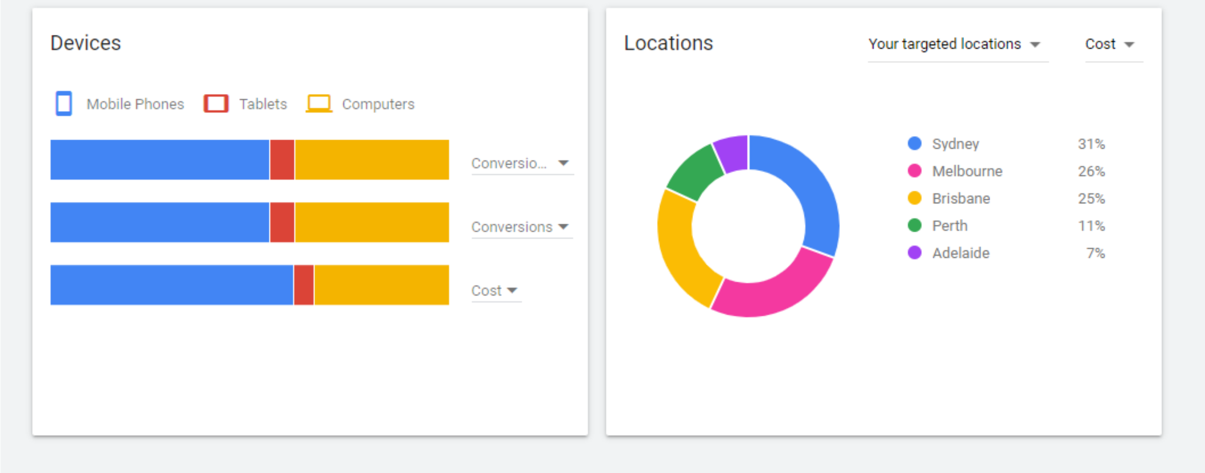
Conversion rate: 5.75%, Value per conversion : ILS66

Conversions	Avg. CPA	Conversion value	ROAS	Clicks	Impressions	Cost	CTR
470	ILS120	ILS31K	0.57	8.1K	140K	ILS54K Daily Budget: ILS2.2K	5.6



Keywords

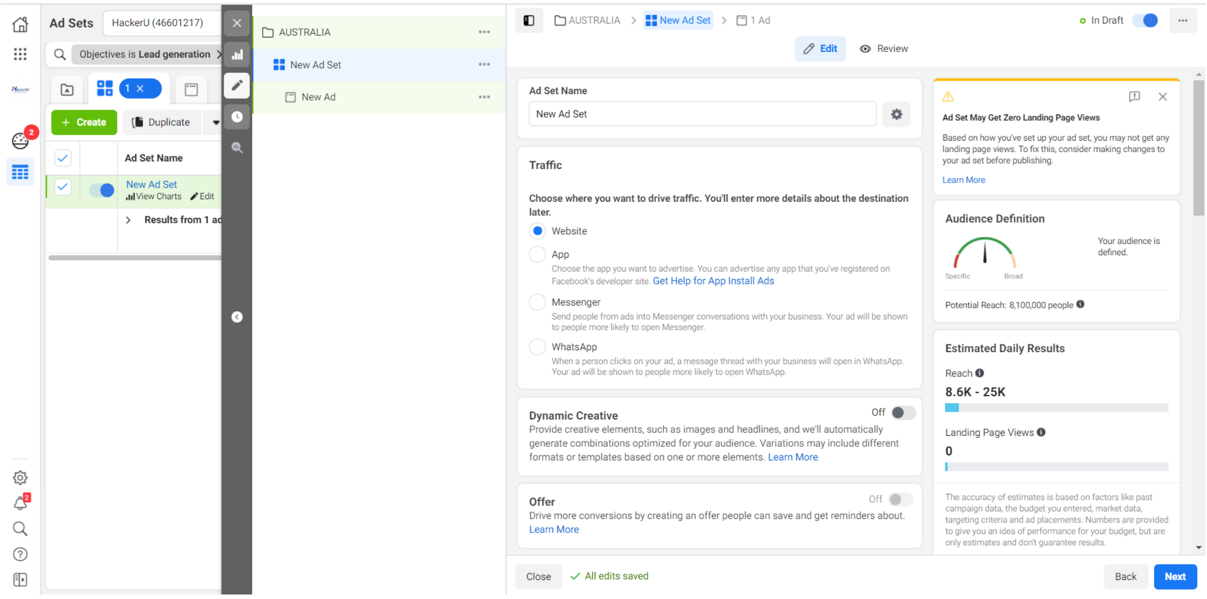
	Conversio...	Conversions	Cost
online courses	ILS19,413.71	294.53	ILS36,844.11
course	ILS4,192.73	63.61	ILS7,071.84
online learning	ILS3,875.10	58.79	ILS4,732.91
online education	ILS3,229.03	48.99	ILS5,108.23
development course	ILS9.18	0.14	ILS11.01



Devices
Mobile Phones
Tablets
Computers
Conversio...
Conversions
Cost
Locations
Your targeted locations
Cost
Sydney 31%
Melbourne 26%
Brisbane 25%
Perth 11%
Adelaide 7%

Appendix C.

Forecasts From Advertising Platforms (Facebook Ads)



Ad Set Name: New Ad Set

Traffic

Choose where you want to drive traffic. You'll enter more details about the destination later.

● Website

○ App
Choose the app you want to advertise. You can advertise any app that you've registered on Facebook's developer site. Get Help for App Install Ads

○ Messenger
Send people from ads into Messenger conversations with your business. Your ad will be shown to people more likely to open Messenger.

○ WhatsApp
When a person clicks on your ad, a message thread with your business will open in WhatsApp. Your ad will be shown to people more likely to open WhatsApp.

Dynamic Creative Off
Provide creative elements, such as images and headlines, and we'll automatically generate combinations optimized for your audience. Variations may include different formats or templates based on one or more elements. Learn More

Offer Off
Drive more conversions by creating an offer people can save and get reminders about. Learn More

✓ All edits saved

Ad Set May Get Zero Landing Page Views

Based on how you've set up your ad set, you may not get any landing page views. To fix this, consider making changes to your ad set before publishing.

Learn More

Audience Definition

Your audience is defined.

Potential Reach: 8,100,000 people

Estimated Daily Results

Reach
8.6K - 25K

Landing Page Views
0

The accuracy of estimates is based on factors like past campaign data, the budget you entered, market data, targeting criteria and ad placements. Numbers are provided to give you an idea of performance for your budget, but are only estimates and don't guarantee results.

Appendix D.

Summary of Forecast Data From Marketing Platforms

Data Type	Google Ads (Ratioed Budget)	Facebook Ads (Ratioed Budget)	Total / Average
Budget (Ratioed)	$18,000.00	$12,000.00	$30,000.00
Estimated Reach	560000	7900000	8460000
Estimated Impressions	140000		8040000
Estimated Clicks	10696	21330	32026
Estimated CPC	$1.68	$0.56	$1.12
Keys	Result		
Google / Facebook Average Ratio	3:2		
Total Budget	$360,000.00		
Monthly Budget	$30,000.00		
Formula	CPC = (Impressions * Historic CTR) / Budget		

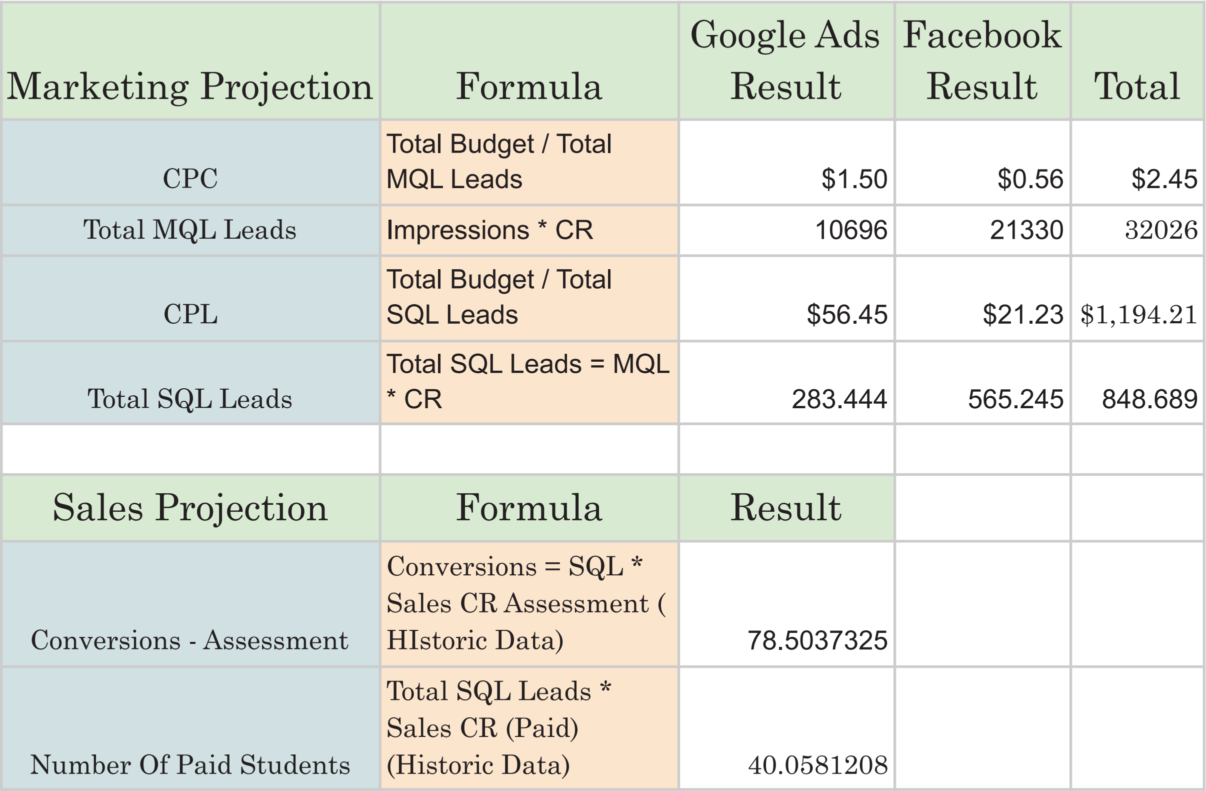
Appendix E.

Metrics Used As Variables Based On Historic Marketing & Sales Performance

Facebook Ads Projections + Historic Data (Variable)	Average Over 2020
Budget	$12,000.00
Impressions	7,900,000.00
Average CTR	0.27%
Google Ads Projections + Historic Data (Variable)	Average Over 2020
Budget	$16,000.00
Impressions	140,000.00
CTR	7.64%
Historic Landing Page Data (Variable)	Average Over 2020
CR (LP)	2.65%
Course Sales Historical Data (Variable)	Average Over 2020
SQL to Free Assessment CR	9.25%
Free Assessment to Paid Student CR	4.72%
Average Sales Cycle Length	3 Months

Appendix F.

Applied Calculations



Marketing Projection	Formula	Google Ads Result	Facebook Result	Total
CPC	Total Budget / Total MQL Leads	$1.50	$0.56	$2.45
Total MQL Leads	Impressions * CR	10696	21330	32026
CPL	Total Budget / Total SQL Leads	$56.45	$21.23	$1,194.21
Total SQL Leads	Total SQL Leads = MQL * CR	283.444	565.245	848.689
Sales Projection	Formula	Result		
Conversions - Assessment	Conversions = SQL * Sales CR Assessment (HIstoric Data)	78.5037325		
Number Of Paid Students	Total SQL Leads * Sales CR (Paid) (Historic Data)	40.0581208		

Appendix G.

Projections Quarter, Year, and 3 Years

Historic Data (Variable)	Average Over 1 Year
Average Sales Cycle Length	**3 Months**
Minimum Students Per Course	**20**
Max Students Per Course	**50**
Time In Course Per Cohort	**12 Months**

	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Number Of Students			40	80	120	160	200	240	280	320	360	400
New Cohort Start / Number Of Cohorts			1	2	3	4	5	6	7	8	9	10
Number of Students Per Cohort			40	40	40	40	40	40	40	40	40	40

	Year 2
Number Of Students	800
New Cohort Start / Number Of Cohorts	20
Number of Students Per Cohort	40

	Year 3
Number Of Students	1200
New Cohort Start / Number Of Cohorts	30
Number of Students Per Cohort	40

Independent Expert Review

Independent Review 1

Cybersecurity Analyst

Amir Khwaja, ACS Member

Amir Khwaja

kamirkamir@gmail.com linkedin.com/in/connectwithamir ☎ +61 4 2020 7669

Professional Summary

An investment banker turned network & cyber security specialist with keen interest in network security and cyber security capable of not only implementing IT security solutions, but also delivering and sharing knowledge through trainings, workshops and formal lectures. Have the capability of leading and managing technical teams in matrix organisations.

Some of the key **career achievements** include

- ✓ Received formal apprecatiation from senior leadership for constantly delivering weekly Cyber Treats Intelligence.
- ✓ Managed portfolios of clients worth more than $100 million and reinvested the money into complex financial instruments such as structured notes and executive bonds using insurance platforms
- ✓ Manged and Train team of upto 12 sales executive and investment bankers with a combined portfolio of $200 million

Core Competencies

- Cyber Security
- Network Security
- Ethical Hacking
- Vulnerability Assessment and Penetration Testing (VAPT)
- Project Management / Account Management
- Training and Awareness.

Work Experience

Cyber Security Analyst (Full -Time Contract)

Jun 2020 to Date

E-Health Queensland Government

Australia (Brisbane)

- Analysed security requirements and assess the needs within customer groups so that a balance between business goals and risk mitigation is realised using information security processes.
- Analysed, specified security requirements and conduct technical security tests to ensure secure and resilient information systems, devices or applications are installed and maintained.
- Ensured that appropriate software and customer documentation is developed to support installed solutions and to ensure a smooth transition into the production environment
- Ensured that proposed information security solutions are in accordance with the organisation's strategic information security direction and utilise the endorsed Corporate methodologies.
- Performed event correlation, monitoring, research, assessment and analysis on enterprise security tools, SIEM, Firewalls, Antivirus systems, proxy devices etc. to gain situational awareness and determine the effectiveness of an observed attack.
- Monitored external data sources (e.g., cyber defence vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defence threat condition Perform initial risk assessment on new threats and vulnerabilities.
- Proactively respond to any potential cyber issues following predefined actions to handle BAU and High severity issues including escalating to other support groups.
- Supported the manager in delivering information security advice and consulting services
- Provided advice and support to the Director, Information Security and Manager, Information Security Solutions about information security matters

Business Trainer and Assessor (Part -Time) 📅 Mar 2020 to Jun 2020

Times Education (RTO) 📍 **Australia** (Brisbane)

- Provided academic trainings on Business students. In addition, ensured that course structure are compliant with the government requirements.
- Instructed through lectures, discussions and demonstrations in campus classroom and virtual classroom.
- Developed detailed daily lesson plans for activities. Worked with an average of 10-20 students per class.
- Used various techniques for teaching students and engaging them in class discussions through case studies, workshops, industry-based lectures and QA sessions, Learning activities and tutorials.

IT Trainer and Assessor (Part -Time) 📅 Jan 2020 to Jun 2020

Australian Institute of Business and Technology 📍 **Australia** (Brisbane)
AIBT - Global (RTO)

- Provided academic trainings on Cyber Security as an IT trainer. In addition, designed courses on IT networking and ensured that they are compliant with the government requirements.
- Instructed through lectures, discussions and demonstrations in IT & Cyber Security.
- Developed detailed daily lesson plans for activities. Worked with an average of 10 - 20 students per class.
- Used various techniques for teaching students and engaging them in class discussions through case studies, workshops, industry-based lectures, learning activity, QA sessions and tutorials.

Cyber Security Consultant (Part -Time) 📅 December 2016 to June 2020

ESS Online 📍 **Australia** (Sydney & Brisbane)

- Lead and managed various consulting projects as a subcontractor to clients such as Vertex, digital innovation in Australia and around the globe.
- Provided corporate trainings on Cyber Security as an IT trainer. In addition, designed courses on IT networking and ensured that they are compliant with the government requirements.
- Provided services to clients for digital transformation of organizations. For example, online establishment and security enhancement.
- Improved clients' networks and websites by conducting audit of their existing IT systems. This includes scanning, analyzing, repairing and advising the clients on the potential cyber security risks.

Business Investment Consultant – Director (Full -Time) 📅 October 2012 – July 2016

Evergreen Businessmen Services LLC 📍 **UAE (**Dubai) **& USA** (Houston)

- Lead and managed various consulting projects as a director of EBS in two locations i.e. Dubai and Houston.
- Designed new financial investment strategies for startups and other branch locations
- Supported startups in setting up their businesses, establishing their IT systems and helped them connect to key stakeholders in the region and around the globe.

Senior Investment Manager (Full -Time) 📅 August 2010 – October 2012

Barclays Bank 📍 **UAE** (Dubai)

- Managed portfolios of clients worth more than $100 million and reinvested the money into complex financial instruments such as structured notes and executive bonds using insurance platforms
- Generated revenue of more than $600,000 for the bank in my individual capacity
- Remained the top investment banker at Barclays for the entire period of employment

Team Manager (Full -Time) May 2008 – August 2010

Royal Bank of Scotland **UAE** (Dubai)

- Remained among the top five investment bankers at RBS
- Achieved the financial targets of the bank beyond the expectations.eg. retained 14 million durhams for six months while the actual target was to retain 5 million durahms for three months.
- Managed team of six relationship managers with a combined portfolio of $200 million.

Higher Education

• Master's in Cyber Security	Australia (Part-Time, In progress)
• Bachelors in Networking (Majors in Cyber Security)	Melbourne Institute of Technology - Australia

Professional Affiliations and Vocational Education

- CEH (Certified Ethical Hacker) – EC Council (Online)
- Diploma in Business – Elite Education (Sydney Campus)
- Cert IV (TA40116) - CBD College (Sydney Campus)
- Member at Australia Computer Society (ACS) #4193748

Independent Review: Cyber Security Analyst for E-Health Queensland Government

Reviewer: Amir Khwaja, ACS Member

1. **The research conducted by HackerU and the need for their Offensive Cyber Security course to be nationally recognised.**

   HackerU's Teach A Man to F.I.S.H. petition nicely defines the current shortage of cyber security talent in the Australian market. It also clearly demonstrates that despite students having relevant qualifications, a lot of them do not have a strong understanding and knowledge of the skills required to secure a job or position after graduation. In connection with this, it is worth noting that HackerU's course proposal highlights the reality of this situation very well in identifying that university graduates often get caught up with updating themselves at the end of their degrees simply because the things which have been taught to them during their first years as students are not relevant in the market. Hence, they still need to enrol with the latest certifications offered by other various institutes and private companies. Additionally, I also endorse with the information cited in the document that the impact of dependency on segments and skills that are imported costs Australian organisations with a lot of money and the choice tomake their own independent decisions.

2. **The vocational and/or educational outcomes of HackerU's proposed Offensive Cyber Security course.**

   HackerU's petition clearly describes the vocational and educational outcomes of their proposed Offensive Cyber Security course. In connection with this, I endorse with the findings of their research that there is currently an industry gap Australia's available courses dedicated to cybersecurity, especially in producing learning outcome(s) where students can come out as jobready graduates who are adequately prepared to join offensive or defensive teams at the onset. Against this background, HackerU's impressive achievements and contributions in the cybersecurity industry looks very promising to address this issue in the Australian market.

3. **HackerU's target group for their proposed Offensive Cyber Security course.**

   HackerU's petition provides a clear description of the target group for their proposed course. That said, I endorse the need for an Offensive Cyber Security course which can be a prerequisite of essential learning from networking or other I.C.T related units to help strengthen the training of cyber professionals in Australia. For all intents and purposes, I definitely endorse that there is a present shortage of blue-team skills and red-team skills within the country, which are much harder to find in the nation's current market. In connection with this, I can share from my own prior experience that an SME can find it difficult to pay an average of $2,000 per day for forensic investigation on a ransomware incident, with no guarantee of deriving results in desired timeframes. If a given business is not cyber-insured, such incidences can destroy a company entirely in just one attack.

4. **The rationale behind HackerU's projected enrolment figures for their proposed Offensive Cyber Security course over the next three years as well as the evidence supporting these figures.**

   HackerU's petition provides a clear rationale detailing the projected enrolment figures for the Offensive Cyber Security course that they are proposing, in addition to supporting evidence that backs up these figures. For the most part, the anticipated demand for their course is in line with the reality that current cyber security training in Australia is mostly related to theory, policy, and compliance; with less focus on hands-on experience of penetration testing done in a simulated work environment. As such, students taking up these courses could end up being frustrated and confused with the process of having to go thru industry/proprietary certification again, like C.E.H. or C.C.N.A. just to get into entry-level jobs within the industry.

5. **The research which HackerU conducted against existing training package qualifications/units of competency relevant to Australia's Cybersecurity industry today, and why these courses are not suitable to meet the needs and outcomes of the organisation's proposed Offensive Cyber Security course.**

   HackerU's petition clearly shows that they have extensively researched existing training package qualifications/units of competency currently available in Australia. Additionally, the document also provides a clear explanation of why these courses are not suitable to meet the needs and outcomes of HackerU's proposed Offensive Cyber Security course. For example, present courses tagged as "Cyber Security" in the country have a significant gap in practical assessments from the N.I.S.T framework or O.S.C.P standards. While these courses have traces of N.I.S.T and O.S.C.P. as introductory theory, unlike HackerU's Offensive Cyber Security course, they miss the actual practical implementation of these frameworks and standards. Furthermore, the majority of growing programming languages within the industry—such as Python or Go, for Automation—are missing in these courses, which can support knowledge about Security Orchestration, Automation, and Response (SOAR).

With specific regard to the subject of the current 22445VIC – Advanced Diploma of Cyber Security, apart from the things mentioned above, it is also worth noting that this course does not cover much about the practical activities that are really done in Red Teams, if its assessment focuses on forensics; compliance; and risk analysis. Last but not the least, I also endorse that it does not teach students the latest requirements needed in the cyber sector like Malware analysis.

Signed ______________________ Date: 26/02/2021

Independent Review 2

Director of Cybersecurity

Sadeed Tirmizey

GSLC, CISM, MACS CP, and ITIL Certified

SADEED TIRMIZEY

Director | Cyber Security | GSLC | CISM | MACS CP

in au.linkedin.com/in/tirmizey
☎ +61 (0) 435 153 147
✉ sadeed@live.com

PROFILE

With an expert understanding of the shifting cyber security landscape and its interconnection with emerging technology, I build high-performance security capabilities that protect both organisational performance and integrity, across the government and private sectors.

Drawing on technical expertise, I bring a proactive approach to risk mitigation, distilling thought leadership and best practice into preventative plans that address emerging cyber security threats. Equally, I understand commercial imperatives and work across stakeholder groups to identify and prioritise needs, bridge interests and identify solutions in the best interest of the business. Seeing security as a critical business enabler, I shift businesses away from reactive ways of working and weave controls into operational BAU. Critically, I instil this same discipline in my teams, building key capabilities, education and knowledge sharing frameworks across multi-stakeholder environments.

Over a career spanning industry (Hewlett Packard, Air New Zealand, ActivIdentity) and large government entities, I have left a legacy of proactive, business partnering cyber security capabilities, providing expertise across security domains. Recently with Queensland Health, I built and matured a greenfield Cyber function that has protected and enabled the agency’s performance, reputation and integrity.

EMPLOYMENT SUMMARY

Director of Cyber Security	Apr 2018 - Present
Chief Information Security Officer (Acting)	Jun 2019 – Feb 2020
Manager Cyber Security (Cyber Defence)	Sep 2016 – Mar 2018
Principal Specialist, Cyber Security	Aug 2011 – Sep 2016
Queensland Health	
Senior Technical Consultant	Sep 2010 – Aug 2011
ActivIdentity	
Technical Security Specialist, Airline Operations	2008 – 2010
Air New Zealand	
Infrastructure Operations Shift Lead	2005 – 2008
Hewlett Packard (HP)	

KEY ASSETS

- **Leader in Cyber Security,** leveraging expertise spanning the digital security and technology risk landscape to formulate and implement cyber-security strategy in complex organisations;
- **Highly developed, interpersonal and stakeholder management skills,** forging relationships across levels and functions to distil complexity and secure buy-in to change programs;
- **Takes a proactive, technology enabled approach to risk management/mitigation,** ensuring appropriate controls are in place to effectively support risk-based decision making;
- **Demonstrable working knowledge across a range of security technologies and frameworks,** incl. NIST Cybersecurity, Mitre ATT&CK, SANS Critical Controls and ISO/IEC 27001/27002;

- **Seasoned in tracking cyber security risk management trends, opportunities and remediation**, advancing organisation's expertise and assessing risk exposure in an evolving landscape.

PROFESSIONAL EXPERIENCE

Director of Cyber Security	Apr 2018 – Present
Chief Information Security Officer (Acting)	Jun 2019 – Feb 2020

Queensland Health

Queensland Health is a branch of the Government of Queensland which operates and administers the state's public health system, employing 83,700 and operating with a $18.3BN annual budget.

- Engaged to mature operational cyber security capability, conducting strategic gap assessments and building required technical skills to transform culture to a proactive approach to risk;
- Lead the design and implementation of a 4-year security road map to develop and deliver a new enterprise-wide cyber security capability, protecting a complex government agency;
- Accountable for $6M OPEX and $2M CAPEX budgets, developing and implementing the annual security operating budget, with a focus on savings targets and operational efficiencies;
- Oversee Information security risk governance, security operations, cyber defence and firewalls (gateways), driving gradual maturity and laying a strong foundation for the future;
- Partner with senior executives and develop key industry partnerships, incl. federal government collaborating to align strategy, identify issues and develop solutions for cyber intelligence;
- Manage a team of 30 incl. 5 direct reports, leading recruitment, career planning, development and performance management, building an engaged and capable cyber security workforce;
- Drive agenda of continuous improvement across Queensland Health, building cyber defence operational security capabilities with embedded cyber threat intelligence function.

Achievements: Director of Cyber Security

- ***Pioneered a new, proactive approach to cyber security, shifting culture*** *and developing and executing a strategy for the design and use of cyber security technology to leadership teams;*
    - ***Champion digital automation to improve cyber security capability,*** *exploring the use of AI to further enable the organisation's ability to detect and prevent threats;*
- ***Delivered a best practice state-wide security service across numerous security domains,*** *aligning with organisational demands, technological trends and industry best practices;*
- ***Continuously matured the cyber defence SOC capability****, identifying and implementing various key initiatives, including Splunk ES upgrade, SOAR, CASB, EPP and EDR implementation in addition to broad operations process improvements;*
- ***Established the Security Working Group to continually align the security agenda and the strategic roadmap,*** *consulting and facilitating stakeholders discussions on key points;*
- ***Improved collaboration between teams and championed a customer-centric approach to solve security issues,*** *streamlining processes and standards of work;*
- ***Boosting the capability of the organisation to efficiently respond to threats and attacks****, cultivating an innovative learning culture and enhancing engagement and morale;*
- ***Strengthened the organisation's security and posture,*** *collaborating with senior stakeholders*

across Queensland Health to implement best practices meeting defined policies and standards.

ACHIEVEMENTS: CHIEF INFORMATION SECURITY OFFICER (ACTING)

- ***Engaged to provide leadership and direction to Cyber Security division of Queensland Health (Jun 2019 to Feb 2020),*** *incl. 17 hospitals & health services, 100K staff and +110K end points;*
    - ***Championed the continued maturity of the cyber security capability,*** *engaging and influencing C-suite, driving delivery of critical cyber security projects valued ~$15M;*
    - ***Developed and led implementation of 5-year 2019 to 2024 Cyber Security Strategy across the organisation,*** *in addition to enterprise wide cyber security programs.*

Cyber Security Manager (Cyber Defence) Sep 2016 – Mar 2018

Queensland Health

- Reporting to the Chief Information Security Officer, promoted to strengthen the organisation's security posture, enhancing incident management capability;
- Designed, developed and implemented 5-year cyber security strategy, overseeing critical cyber security improvement projects and programs, managing within the allocated budget;
- Provided leadership to 12 direct reports on the cyber defence team, implementing a 'people first' approach to facilitate engagement, high-performance and boost morale;
- Built and managed relationships with key stakeholder during a significant period of change, incl. senior managers, technical teams, customers, governing committees and working groups.

ACHIEVEMENTS

- ***Created a foundational level of operational capability to proactively identify cyber threats,*** *developing processes to integrate intelligence continuously assess of possible threats;*
- ***Established the first 24/7 cyber security operations centre,*** *creating the Cyber Defence Wing (SecOps, CTI, IR, VMS, threat hunting) and managing the Cyber Security Operations Centre;*
- ***Identified key areas of improvement and developed a long-term strategy following the G20 summit,*** *conducting a gap analysis on risk assessment with Chief Information Security Officer;*
- ***As a result, developed and delivered business critical cyber security projects and programs*** *incl. the Customised Cloud Security Risk Assessment model and security assurance program;*
- ***Developed and implemented a customer-centric approach to governance,*** *establishing an approachable form of security policies and guidelines in partnership with key stakeholders;*
- ***Embedded continuous improvement culture to meet benchmark and industry standards,*** *systemically reviewing processes and security standards at regular intervals.*

Principal Specialist, Cyber Security Aug 2011 – Sep 2016

Queensland Health

- Responsible for providing strategic oversight from an Information security perspective for new hospitals programme, reporting to the Director of Information Security;
- Developed and contributed to the overall cyber security strategy, providing high-level support and consulting to project managers driving the Information Security Risk Assessment process;
- Led the provision of high-level Information Security advice, consulting services, infrastructure matters and design review, delivering expertise and support to senior management.

ACHIEVEMENTS

- ***Added value to the organisation by transforming the compliance-based approach to cyber security,*** *conducting risk-based assessments to identify issues and review processes;*

- ***Strengthened the organisation’s cyber defence capability, establishing and managing the Cyber Security Incident Response capability** and implementing the Information Security Incident Management Standard and the Response Procedure;*
- ***Led end-to-end cyber security reviews for major projects including University Hospital Queensland and Children’s Hospital Queensland,** managing through the design phase;*
- ***Streamlined security review and engagement processes,** establishing the Cyber Security’s Customer Engagement process in line with strategic goals and objectives.*

Senior Technical Consultant Sep 2010 – Aug 2011

ActivIdentity

ActivIdentity is an authentication and credential management company that provides identity solutions for digital interactions, employing ~50 and generating $11M in revenue per annum.

- Engaged following contract win with a key government client to identify and eliminate security loopholes, ensuring the new Smart License was protected from fraud and identify theft;
- Supervised project progress and provided technical guidance to the on-site technical consultant, identifying solutions to complex issues throughout the project;
- Managed responses to security incidents, incl. SCMS Logical Access and Identity Assurance;
- Provided security consulting across data loss prevention, deployment of data protection and privacy solutions and enterprise rights management, monitoring via security audits.

Achievements

- ***Delivered the New Queensland Driving License Project upgrading to a more secure Smart Card** with enhanced security features including facial recognition, partnering with client on site;*
- ***Secured a large financial windfall for the company having successfully delivered the Driving License Project,** managing relationship and release of payments to ActivIdentity;*
- ***Effectively analysed and identified security issues**, deploying selected technologies showcasing general awareness of the trends and issues in Information Security.*

Technical Security Specialist, Airline Operations Apr 2008 – Sep 2010

Air New Zealand

The flag carrier airline of New Zealand, employing +10K and generating ~$5.2M in revenue p.a.

- Responsible for supporting security, availability and reliability of IT infrastructure in a multi-platform integrated environment, underpinning the day to day operations of the airline;
- Collaborated with key stakeholders as a member of the Change Advisory Board.

Achievements

- ***Ensured a consistent ITIL based approach for all areas of Group IT service management,** via the establishment and promotion of best practices within IT service delivery;*
- ***Improved resilience and minimised security risk to airline operations**, guaranteeing security requirements for critical system continued to be met via hardware upgrade projects;*
- ***Developed, tested and executed disaster recovery plans for high severity system**, supported by new and continuously updated security policies for airline operations IT systems.*

Lecturer – Department of Computing | ***UNITEC New Zealand*** 2009 to 2010

Infrastructure Operations Shift Lead | ***Hewlett Packard (HP)*** 2005 to 2008

EDUCATION

Post-Graduate Diploma, Computing	UNITEC New Zealand
Bachelor of Business Administration	University of New Brunswick

PROFESSIONAL DEVELOPMENT

Certified Professional ACS	Australian Computer Society
GIAC Security Leadership Certification	SANS
Certified Information Security manager	ISACA
ITIL v3 Certification	British Computer Society
Incident Response Team Management	SANS
Security Leadership Essentials	SANS

References available on request

Independent Review: Director of Cyber Security for Queensland Health

Reviewer: Sadeed Tirmizey, GSLC, CISM, MACS CP, and ITIL Certified.

1. **The research conducted by HackerU and the need for their proposed Offensive Cyber Security course to be nationally recognised.**

   From my own experience, the current Australian market is suffering from a significant shortage of suitably qualified cyber professionals. The sector requires Cyber Security professionals with a strong foundational knowledge of cyber security and the industry's evolving landscape. After extensively reviewing HackerU's petition and the evidence they presented, I am satisfied that they have undertaken sufficient research which clearly confirms the need for their proposed course to be nationally recognised.

2. **The vocational and/or educational outcomes of HackerU's proposed Offensive Cyber Security course.**

   HackerU's petition presented information clearly about the desired outcomes of the Offensive Cyber Security course that they are proposing. I am confident that this course and the topics covered by it will contribute to preparing members of the workforce which are ready to participate and contribute to the cyber defense strategies of different organisations.

3. **HackerU's target group for their proposed Offensive Cyber Security course.**

   HackerU's petition provides sufficient information about the target group of the Offensive Cyber Security course that they are proposing. Having been in the cyber industry for over 10 years, I have noticed and experienced a gradual decline in the quality of security professionals coming into the industry. This is despite a strong interest in the cyber security sector across the student community. For the most part, this continued shortage of quality local security professionals can be attributed to the lack of sufficient training and education options available in the market.

4. **The rationale behind HackerU's projected enrolment figures for their proposed Offensive Cyber Security course over the next three years as well as the evidence supporting these figures.**

After reviewing the data presented by HackerU, I am satisfied that the projected enrolment figures which they have identified are in line with current available information, as well as projected demands within the cyber security sector. As an expert in the industry—and in view of the things that I've seen in numerous discussions amongst various groups and forums—I have observed growing interest in the cyber sector and HackerU's projected industry demand is consistent with my expectations.

5. **The research which HackerU conducted against existing training package qualifications/units of competency relevant to Australia's Cybersecurity industry today, and why these courses are not suitable to meet the needs and outcomes of the organisation's proposed Offensive Cyber Security course.**

HackerU's course proposal has been clearly researched and based on the information they presented, it is clearly evident that the existing Certificate IV and Advance Diploma courses currently on offer in the market do not comprehensively cover the topics which are required to understand and respond to the continuously evolving threat landscape of the Australian cyber sector. At the moment, organisations within the country are presently experiencing a significant shortage of suitably qualified and trained cyber professionals.

In the contemporary cyber threat landscape, professionals are required to be familiar with the end to end security spectrum, along with having a strong foundational understanding of cyber security. The pervasive piece meal approach of training professionals only in selected sections is definitely not suitable and places great burden on organisations to upskill new starters.

Signed

Date: 24/2/2021

Independent Review 3

Cyber Consulting Manager, UNSW

Chadi Maurad

CISSP, CISM, CISA, CRISC, CDPSE, SABSA, and ITIL Certified

CHADI MOURAD

56 Unwin Street, BEXLEY, NSW, 2207· **0413274647**
Mouradc123@gmail.com
https://www.linkedin.com/in/chadi-mourad-6ab2a58/

Results-driven Senior IT Security Expert with proven ability to protect vital systems from internal and external threats. Demonstrated leadership skills that guide teams towards success and drive businesses towards excellence. Strong communication and organizational skills, ability to multi-task, strong attention to details and excellent problem solving. Dedicated to remaining current on security developments to ensure that effective preventative measures are taken to reduce risk.

EXPERIENCE

MAY 2018 - CURRENT

SECURITY CONSULTING MANAGER, UNIVERSITY OF NEW SOUTH WALES (UNSW)

Manager for security consultancy in UNSW since July 2019.
Product owner for the UNSW Data Loss Prevention (DLP) and Information protection (AIP) systems across the entire university.
Product owner for the UNSW Cloud Access Security (CASB) system.
Support the implementation of the Governance Risk and Compliance (GRC) suite of tools, build GRC processes and workflows for different parts of the University (Risk, Compliance, vendor management, Threat and Vulnerability management and Enterprise risk).
Lead the University to obtain a membership to the Defence Industry Security Program (DISP).
Working on a 5-year Cyber Transformation Program that includes setting the security strategy in alignment with the University's 2025 strategy, reviewing the security policy and standards to ensure support for the new strategy, creating a Cyber Risk strategy and processes and a number of security initiatives.
Serve as the principal cyber strategic advisor and subject matter expert to brief stakeholders and executives at the highest levels within the university.
Oversee the development of proposals, business cases to ensure alignment with Cyber Strategy.
Creating security guardrails for new ways of working between the UNSW project management office and Cyber security.
Inform, advise, and participate in executive cross-functional and security steering committees related to cybersecurity capabilities to protect against cyber threats.
Negotiated contracts with vendors, built and maintained positive working relationships with external suppliers and stakeholders.
Assist in the development of an IT Risk Management framework and processes.
Project engagement and providing expert IT security advise and change implementation requirements of UNSW IT, Faculties, Divisions, Affiliate, and stakeholders.
Perform risk assessments during project engagements and ensure that security risks are communicated, recorded, eliminated, mitigated, or accepted by appropriate levels of business management.

FEB 2019 – SEP 2020 (PARTTIME)

SENIOR SECURITY CONSULTANT, XINJA BANK

Lead the bank's PCI-DSS compliance program.

Performed security related activities to assist the bank in obtaining a banking license from APRA.
Designing and applying a mature third-party security evaluation assessment process to meet the bank's compliance requirements.
Product and program security assessments.

JAN 2012 – APRIL 2018

SECURITY LEAD – IT CUSTOMER SERVICE MANAGER, ORANGE BUSINESS SERVICES

Winner of the Australasian employee of the year award in 2012.
Security service ownership, responsible for the Operational Management of Security Services for large enterprise customers in the mining industry.
Delivery of the global Security Management team into the assigned accounts.
Acting Manager for IT Customer Service Management in the region.
Achieving customer satisfaction that led to the renewal of a major contract for security services.

MAY 2004 – JAN 2012

SENIOR INFORMATION SECURITY CONSULTANT, THE WESTPAC GROUP

SENIOR SECURITY CONSULTANT, ST GEORGE BANK LIMITED

Implementation and maintenance of the security infrastructure to protect the business from security breaches, this includes a wide variety of security services including but not limited to Firewalls, load balancing, IPS system implementation, configuration, maintenance, and documentation.
Network management for multiple site configuration running different network technologies.
Security Standards creation and administration.
Provide information security oversight and governance services to the Westpac Group.
Responsible for the Secure by Design (SBD) certification which is a process to assess the effective security posture of a project.
Performed Security Due Diligence on Third Party vendors for offshoring arrangements.

JULY 2000 – MAY 2004

SECURITY/ WAN SPECIALIST, SYNTEGRA/ HANSEN TECHNOLOGIES

Third level support for large Financial and Government customer-based networks.
Duties include router/ switch inter-network, Firewall log tracking, defining firewall rules, objects, and users, applying patches and system maintenance. (Customers including ING Bank, Baycorp, Australian Central Credit Union, Combined Financial Processing (80 different Credit Unions with 250 Branches), Illawarra Credit Union, Tasmanian Credit Union, Island State Credit Union and many more).
Responsible for managing the Network Services Team consisting of 15 LAN/ WAN/ Security specialists. Bid approvals, leave applications, on-call rosters and overtime forms.
Delegation of activities related to projects, bids, presales activities, day to day activities like network maintenance and faults.

EDUCATION

Certified (In good standing): CISSP, CISM, CISA, CRISC, CDPSE, SABSA and ITIL.
Extensive training in different security products including: F5, Radware, Juniper, Checkpoint, Palo Alto, Cisco, Netscreen, Zscaler, BlueCoat, AWS, and Microsoft products and services.

SKILLS

- Cyber security management
- Incident security management
- Cyber strategy and governance
- Critical system evaluation
- Security service management
- Cyber security consultancy
- Risk assessment and management

Independent Review: Cyber Consulting Manager for the University of New South Wales (UNSW)

Reviewer: Chadi Mourad, CISSP, CISM, CISA, CRISC, CDPSE, SABSA and ITIL Certified

1. **The research conducted by HackerU and the need for their Offensive Cyber Security course to be nationally recognised.**

   It is a well-known fact within the Cyber security industry that Cybercrime is always on the rise, with figures showing that Australians reporting cyber security incidents every 10 minutes, and costing businesses $29 billion each year. Consequently, it is evident that there is an increased demand for cyber security specialists to develop systems that offer safety and security for businesses and everyday Australians who are reliant on digital platforms. It is also evident in recent Media reports that Australia is facing a skills shortage of 18,000 cybersecurity experts by 2026 as the nation fights unprecedented attacks on business, government, and critical infrastructure.

   A surge in malicious activity revealed by Prime Minister Scott Morrison recently has highlighted the training gap, with coronavirus border closures squashing the ability to import experts. Based on my own experience in the industry, it is always difficult for me to find strong candidates for Cyber Security job vacancies.

   The industry is projected to almost triple in size by 2026 and requires an estimated 16,600 additional professionals in both technical and non-technical cyber security positions. The education sector is responding with course offerings, from Graduate Certificate through to Post-Doctoral levels, albeit not at a pace that meets the market and there are always training gaps.

   The Teach A Man To F.I.S.H program is designed for individuals that want to help in providing safe and secure online experiences, often to some of the most vulnerable online users and for those who want to further develop expertise and diversify career options.

   There is detailed evidence in the Teach A Man To F.I.S.H. petition that research has been undertaken based on surveys, official government reports and documents, It clearly highlights why we need for the course to be nationally recognized and specifically to assist us in bridging any training gaps and growing the industry to meet with the forecasted demand.

2. **The vocational and/or educational outcomes of HackerU's proposed Offensive Cyber Security course.**

The outcomes of the proposed course are clearly described, it shows how the course will assist Australia in addressing the cyber security industry's skilled workers shortage and provide economic benefits to the country. It also shows the training gaps in the existing source offerings and how this course will bridge these gaps.

As an expert in this industry, the trends from the environments that I am responsible for managing show us that the sophistication and the number of Cyber-attacks is always on the rise. Finding good candidates for job openings is always difficult.

The outcomes of this course meet the Australian Cyber Security's need to respond to the increase in Cyber-attacks. The industry is projected to require an estimated 16,600 additional professionals by 2026 that need to be trained to achieve new skills in Cyber Security. These training needs cannot be met by current training package qualifications.

3. **HackerU's target group for their proposed Offensive Cyber Security course.**

The course will attract a diverse cohort and is designed for a broad audience. It is designed to attract students from diverse backgrounds. Women, Minorities, Older Aged, and those from a lower social-economic demographic are largely represented in contrast to a traditional IT cohort. This training is suitable for all people or groups including students, employees, contractors, and volunteers. As more and more people are now online, Cyber Security is an interesting topic to everyone. Conversations which I have had with many people show this—and not necessarily just people from the IT industry. People always want to know, how do I become a Cyber Security expert? And what training do I need?

4. **The rationale behind HackerU's projected enrolment figures for their proposed Offensive Cyber Security course over the next three years as well as the evidence supporting these figures.**

Based on many available public sources, the cyber security industry is projected to almost triple in size by 2026 and requires an estimated 16,600 additional professionals in cyber security positions, most of which will be seeking training and upskilling.

The length of HackerU's proposed Offensive Cyber Security course will be most appropriate to the needs of the target group of learners who want to gain skills quickly without doing a full university degree over a period of 3 to 4 years. Since

Teach A Man To F.I.S.H only consists of 13 modules and requires just 625 hours, the course will help in producing trained staff for the market in a shorter timeframe.

5. **The research which HackerU conducted against existing training package qualifications/units of competency relevant to Australia's Cybersecurity industry today, and why these courses are not suitable to meet the needs and outcomes of the organisation's proposed Offensive Cyber Security course.**

   HackerU's proposed Offensive Cyber Security course covers a wide area of security, ranging from Operating System to the perimeter environment. It also focuses on the topic of how to compromise such environments and has a practical hands-on component in its training delivery. With that being said, gaps in existing training packages available in the market today have been clearly researched by HackerU and detailed in their petition document. Additionally, it also clearly outlines how their proposed course will address these gaps and shortcomings.

Signed

Date:

24/2/2021

Independent Review 4

RTO Auditor

Gizette Cao

Senior VET Compliance Specialist

Gizette is one of 360RTO Solutions' lead auditors and is a skilled "RTO Lifeguard" that has saved countless RTOs by enhancing their compliance. She has completed a huge number of audit and rectification projects, and delivers a number of compliance consultations nationally, across a variety of RTO topics.

Gizette Cao

Education

- TAE40110 Certificate IV in Training and Assessment – 2015
- TAE50111 Diploma of Vocational Education and Training – 2016
- TAE50211 Diploma of Training Design and Development – 2016
- TAE50216 Diploma of Training Design and Development – 2020
- Bachelor's Degree in Nursing / Registered Nurse

Experience

- **Compliance Team Leader and Lead Auditor at 360RTO Solutions**
  2017 – present

  Core Service Offerings: VET Regulatory Compliance, Compliance Audits, Process Improvement, Program Development, Launch and Implementation, Quality Assurance, RTO, CRICOS, ELICOS Registration
  - Reports to the Managing Director
  - Product and process development for RTO consulting services: Audit, Rectification, CRICOS, ELICOS, Addition-to-scope Registrations
  - RTO product development: Training products, training and assessment strategies, compliant learning and assessment resources, policies and procedures, compliance documents
  - Audit preparation: facilitating workshops on ASQA standards and compliance for RTO operators, conducting simulation of full ASQA audits, rectification, risk management, preparation/development of compliance documents, review and update RTO policy and procedures to align with the Standards for RTOs 2015, and overall quality assurance
  - Registration: Development of RTO systems and processes, training products, policies and procedures, systems and tools to facilitate operational compliance and ongoing quality management activities, preparation of application and application requirements for initial registration, addition to scope, CRICOS and ELICOS applications, including preparation for relevant audits

  - Ongoing compliance: facilitate validation and moderation activities; identify, initiate and implement continuous improvement opportunities; manage create and deliver staff professional development and compliance training; develop and maintain trainer and assessor skills matrix and professional development register; assist clients with cooperating with the national VET regulator

- **Training and Assessment Team Leader at Inspire Education (RTO 32067)**

  2014 – 2017

  - Overseeing the day to day tasks of TAE trainers and assessors, ensuring activities meet targets, and training and assessment is delivered according to the Standards
  - Providing training and support to new TAE trainers and assessors
  - Fostering collaborative work practices and promote a workplace environment focused on staff empowerment, efficient work practices and encouragement of initiative and innovation
  - Training and Assessment: train and assess students enrolled in Certificate IV in Training and Assessment, Diploma of Vocational Education and Training, and Diploma of Training Design and Development
  - RPL Specialist: assess RPL submissions for Certificate IV in Training and Assessment, Diploma of Vocational Education and Training, and Diploma of Training Design and Development

- **Senior ESL teacher / Team Leader**

  2010 – 2014

  - Prepare materials for class activities
  - Instruct students (face-to-face) individually and in groups, using various teaching methods such as lectures, discussions, and demonstrations
  - Adapt teaching methods and instruction materials to meet students' varying needs, abilities, and interests
  - Observe and evaluate students' work to determine progress and make suggestions for improvement
  - Make progress report of students

Independent Review: RTO Auditor and Registration Consultant for 360RTO Solutions

Reviewer: Gizette Cao, Senior VET Compliance Specialist

1. **The research conducted by HackerU and the need for their Offensive Cyber Security course to be nationally recognised.**

   After reading HackerU's course proposal, I can positively state with a strong degree of confidence that they have performed a sufficient amount of research and investigation while drafting their petition. In addition to this, following the application of subjecting the details of their proposal to an extensive validation and review process—with the aim of assessing the validity and relevance of the various reports and sources of information that they have cited and referenced—I can accordingly endorse that the data and evidence which HackerU has provided to corroborate the arguments of their petition are credible. Against this background, taking into consideration the collective body of supporting documentation that they have presented, I can thus decisively declare that HackerU's course proposal presents a pretty strong case for the national recognition of the Offensive Cyber Security course that they are aiming to get accredited.

2. **The vocational and/or educational outcomes of HackerU's proposed Offensive Cyber Security course.**

   Upon reading and reviewing HackerU's "Teach A Man to F.I.S.H – Petition to Accredit" document, I was able to quickly verity and confirm that HackerU has clearly defined and outlined the vocational and educational outcomes of their proposed Offensive Cyber Security course.

3. **HackerU's target group for their proposed Offensive Cyber Security course.**

   Upon reading and reviewing HackerU's "Teach A Man to F.I.S.H – Petition to Accredit" document, I was able to quickly establish and verify that they have clearly presented and described the target group and prospective students of the Offensive Cyber Security course that they are aiming to get accredited.

4. The rationale behind HackerU's projected enrolment figures for their proposed Offensive Cyber Security course over the next three years as well as the evidence supporting these figures.

Upon reviewing and examining HackerU's "Teach A Man to F.I.S.H – Petition to Accredit" document, I was able to clearly see and verify that they have outlined and presented a detailed rationale behind their forecasted enrolment figures for their proposed Offensive Cyber Security Course. In addition to this, I was also able to confirm that they have provided valid and convincing evidence to support their projections.

5. The research which HackerU conducted against existing training package qualifications/units of competency relevant to Australia's Cybersecurity industry today, and why these courses are not suitable to meet the needs and outcomes of the organisation's proposed Offensive Cyber Security course.

After assessing and evaluating HackerU's "Teach A Man to F.I.S.H – Petition to Accredit" document, I can confirm and attest that they have performed their research regarding the existing training packages and courses currently listed and identified in Australia's National Register for Cyber Security. In connection with this, the details of the Technical Course Comparison section presented in their proposal, clearly showcases that they have extensively given and outlined multiple critical reasons as to why current VET training packages in the country do not meet the practical learning and vocational outcomes of their proposed Offensive Cyber Security course.

Signed

Date: 26/02/2021

Independent Review 5

RTO Compliance Consultancy Director

Brent Rogers

VET Compliance Expert, RTO Owner

With extensive professional experience in running a range of private companies since 2000, Brent has a deep understanding of the commercial and market realities of running small through to large RTOs, as well as an understanding of how to develop “turn key” business systems and processes to ensure sustainable growth, solid professional development in staff, and to gain maximum efficiency.

Brent is the Managing Director of one of Australia’s Leading professional RTO Consultancy & Recruitment companies, 360RTO Solutions – providing affordable professional RTO services, including new RTO registrations, and a huge range of cost-effective, compliance-enhancing professional services that ensure robust ongoing compliance for small, medium, and large RTOs around Australia.

Education

- Bachelor Of Psychological Science w/ Honours, Psychology, Distinction – 2013
- Certificate of Therapuetic Massage / Certificate of Aromatherapy, Massage Therapy, Aromatherapy – 1999
- Certificate IV in Training and AssessmentField Of StudyTraining and Assessment

Experience

- **Director – 360RTO Solutions**
  Feb 2015 – Present

  Managing Director of one of Australia's Leading professional RTO Consultancy & Recruitment Companies, 360RTO Solutions.
  360RTO assists with new RTO registrations, and offers a range of robust, cost-effective professional compliance services and solutions to ensure robust ongoing compliance for small, medium, and large RTOs around Australia.

  As one of Australia's largest dedicated RTO recruitment services, 360RTO understands the needs of the RTO industry in a unique and hands-on way. Management has owned and managed RTOs for over a decade, understanding every role, and its unique requirements as part of the VET industry.

  Helping to drive strong Quality, Compliance, Efficiency, and Profitability is the mission of our organisation. 360RTO is quickly becoming the market leader for RTO start-ups and well-established RTOs desiring high-quality professional services and compliance without the huge pain and expense that would otherwise be involved.

- **Owner – Inspire Education Pty Ltd**
  Jan 2009 – Present

  Co-owner of one of Australia's largest RTOs, services over 10% of all Australian Certificate IV in Training and Assessment enrolments, and delivery training nation-wide across over 20 high-demand qualifications.

- **Managing Director/Principal – Inspire Education Pty Ltd**
  Jan 2009 – Oct 2016

  Managing director and strategist of a leading Australian provider of vocational training, Inspire Education (www.inspireeducation.net.au) that serviced over 20,000 students through this period. Inspire is a leading provider of the 'flagship' qualification of the VET industry - the Certificate IV and Assessment. Other leading qualifications include work health and safety (WHS), TESOL (teaching English to Speakers of Other Languages), management, HR, business, administration, financial services, child care, community care.

  As Managing Director my responsibilities also included:
  - Strategic planning and direction for all major departments (independently, and assisting key managers/coordinators)
  - Developing, coaching, and supporting key managers, and their systems and processes (in RTO operations; administration; student services; training; HR; recruitment; marketing; and sales)
  - Creating HR systems and processes in line with established organisational psychology principles, and to ensure trainer compliance
  - Developed, implemented and trained in best recruitment practices - including psychometric testing, behavioural interviews, and recruitment monitoring, systems and processes
  - Helped ensure RTO compliance in a range of areas - including internal auditing, and creation of tools, policies, procedures, and compliance management systems
  - Created, co-created, and edited a range of tools, policies and procedures to ensure compliance with the National Standards for RTOs.
  - Researching and exploiting new market opportunities
  - Guiding the product development priorities
  - Deep data crawl and analysis to predict trends, forecast, and adjust business model/products to changing market conditions
  - Allocating and monitoring the marketing and advertising budget it to ensure it met objectives
  - Creating, implementing, and guiding maintenance of online marketing platforms, automation, and tools
  - Reviewing reports and regularly meeting with key managers

- **Director – Future Communication Solutions**

  May 2000 – Dec 2008

  Recruitment, selection, induction, and coordination of staff
  Drafting and execution of employment contracts
  HR/Industrial relations
  Staff reviews and assessment
  Workforce planning

  Strategic planning of business development opportunities, product launches, and marketing campaigns
  Critical analysis or campaign viability and budget monitoring
  Costing, forecasting, and analysis

  Liaison between Future Communication Solutions and telecommunications service providers
  Contract negotiations
  Needs analysis with business and corporate clients to determine appropriate solutions
  Corporate clients liaison and client relationship maintenance
  Opening new accounts for existing and new customers
  General account maintenance
  Assisting customers with complaints
  Creating opportunities with business partners and resellers

  Coordination and training of sales and marketing team
  Managed team of 20+ sales consultants
  Offline and online marketing planning and execution
  Meeting key marketing/sales objectives and budgets
  Forecasting

- **Sole Proprietor / Massage Therapist – Utopian Dreams**

  Nov 1998 – May 2000

  Utopian Dreams produced handmade natural cosmetics using using pure essential oils, crystrals and jewellery targeted at customers who preference natural health and spiritual pursuits.

  As well as running a stalls and selling these goods at venues and exhibitions throughout Auckland and New Zealand, I also performed massage and natural therapies aimed at promoting relaxation, wellness, and health maximisation.

- **Independent Contractor – Souther Elecric**

  Oct 1997 – Oct 1998

  Independent contractor and sales consultant for leading electricity and natural gas supplier in the United Kingdom, including the management of a subcontractor who worked with me.

  My role was to independently source and acquire clients right across the United Kingdom to aid them in making the transition to a more cost-effective gas and electricity solution with Southern Electric.

  Skills employed on a daily basis were customer acquisition, negotiation, up-selling, and building a client referral network. Additionally, I trained my subcontractor in the sales process and how to successful negotiate with clients. My strong results repeatedly demonstrated my aptitude in the area of client relationship building and business development.

Independent Review: Director – Strategy & Growth for 360RTO Solutions

Reviewer: Brent Rogers, VET Compliance Expert and RTO Owner

1. **The research conducted by HackerU and the need for their Offensive Cyber Security course to be nationally recognised.**

   As a VET Compliance Expert and RTO Owner, after closely reviewing HackerU's course proposal, I can confidently confirm that they have certainly done their homework in researching the current status quo of Cybersecurity Education in Australia. In relation to this, taking into consideration the critical data and information outlined within the reports cited in their petition, I am strongly convinced that there is indeed an urgent need and exigency for their proposed Offensive Cyber Security course to become nationally recognised, given the documented skills shortages within our country's Cyber Sector as well as the potential economic advantages and benefits which may be brought by the prospect of further strengthening and developing this vital component of our nation's industry.

   From my own personal experience, as a Business Owner myself, I can definitely attest to the fundamental importance of data and cyber security in the running of my own group of companies. Being directly involved within the VET sector, it goes without saying that the protection and safety of all of the data and sensitive information of each of the students, staff, and clients—involved and dealing with my organisations—are always at the top of my priorities. With that being said, I regularly receive reports from my own I.T. teams about phishing and hacking attempts from malicious individuals seeking to attack and compromise the digital security of my companies. Against this background, I firmly support HackerU in their mission and endeavour to help grow and produce more Cyber Security professionals in our country.

2. **The vocational and/or educational outcomes of HackerU's proposed Offensive Cyber Security course.**

   As a VET Compliance Expert and Owner of one of Australia's largest RTOs, after reviewing HackerU's Teach A Man to F.I.S.H petition document, I can strongly attest and confirm that the vocational and educational outcomes of the Offensive Cyber Security course that they are seeking to accredit are clearly outlined in their proposal. In relation to this, I also want to note that I can clearly understand and envision the practical learning and skills-related outcome of the course concept which they are proposing.

3. **HackerU's target group for their proposed Offensive Cyber Security course.**

   HackerU's petition document clearly identifies that the targets for their proposed Cyber Security course will be directed towards individuals from diverse backgrounds; including women, minorities, older persons, and individuals coming from a lower socio-economic demographic. With that being said, in view of the consideration that a shorter VET Offensive Cyber Security course will clearly be more affordable and accessible to most of individuals than a full 3 to 4 year university degree, I definitely believe in the prospect and expectation that their course will be a hit and success in these given sections of the market.

4. **The rationale behind HackerU's projected enrolment figures for their proposed Offensive Cyber Security course over the next three years as well as the evidence supporting these figures.**

   Upon reviewing HackerU's petition document, I can clearly understand and grasp the rationale behind projected enrolment figures outlined in their proposal. As a Business Owner who has over 25 years of experience in sales and marketing—based on the budget which they will be allocating for their advertising and promotional campaigns, the demographics of their target markets, as well as the historical performance data which they have presented from their past marketing activities—I can confidently confirm and endorse that HackerU's forecast for their proposed course's anticipated admissions are in line with realistic expectations and the findings of my own personal assessment.

5. **The research which HackerU conducted against existing training package qualifications/units of competency relevant to Australia's Cybersecurity industry today, and why these courses are not suitable to meet the needs and outcomes of the organisation's proposed Offensive Cyber Security course.**

   Upon reviewing HackerU's petition document, I was able to clearly see and verify that HackerU certainly conducted extensive research and assessment of the existing VET qualifications and courses for Cyber Security that are presently available in the Australian market. In connection with this, the technical comparison which they have made between their proposed Offensive Cyber Security course against these aforementioned qualifications and training products unambiguously showcases and highlights the distinction of the specialised course that they are currently putting forward for accreditation. For all intents and purposes, as evidenced by the comprehensive and exhaustive details of HackerU's analysis on their petition document, I strongly agree with their points and findings regarding the failure of existing Cyber Security qualifications and training products on offer today to meet and address the critical learning and skills outcomes which their proposed Offensive Cyber Security course intends to provide to students.

Signed

Date: 26 February 2021

Thank You

For Your Consideration