F.I.S.H.

- Future
- In digital
- Security
- Human resources

Teach a Man To F.I.S.H. Initiative

An initiative to export Israel's core factor for its cybersecurity excellence, for Australia’s industry to blossom

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. Hacker 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 & Methodology

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

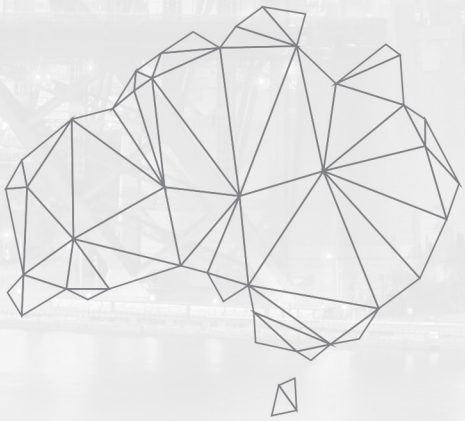
Supporting research Documents (But Not Quoted) Include:

- 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.

Sponsored by: *HackerU Global Education*

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	**48.4%**	**- 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:

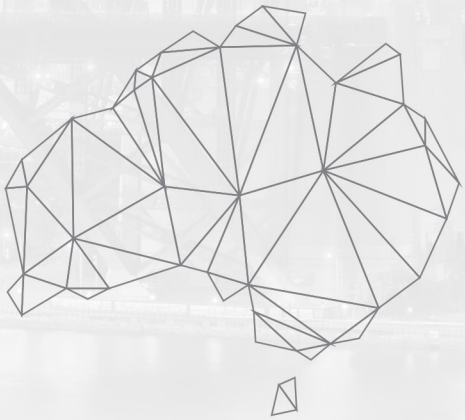
"Roughly three quarters of the global expenditure on cyber security comes from cyber security 'users' (organizations and Individuals seeking to defend themselves against malicious cyber activity) purchasing the products and services of external cyber security 'providers' (both specialist cyber security 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%**

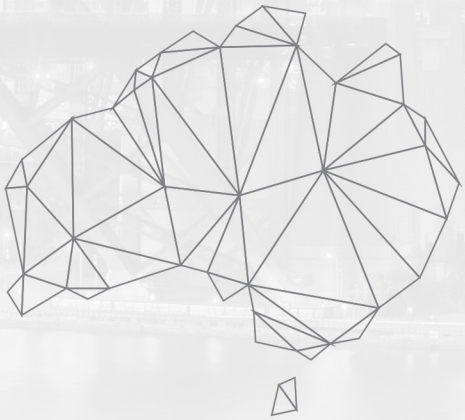
Recruitment Time	**20 % - 30 % Longer Than Average**

> ***"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.