www.pwc.com.au

Public Paper

Cyber Security Cross Sector Project

PwC's Skills for Australia

November 2017

pwc

Foreword

The shortage of Cyber Security talent is a challenge for every industry sector globally. Demand for Cyber Security professionals is fast outpacing the supply of qualified workers. In Australia, 88% of businesses believe there is a significant shortage of Cyber Security professionals in the country and the continued skills shortage could leave organisations more vulnerable to cyber attacks.[1]

The Australian Industry and Skills Committee (AISC) has taken the opportunity to strategically address common skills needs – current and future – across multiple industries through eight cross sector projects. These eight common skills areas have been identified by various Industry Reference Committees (IRCs) in their Industry Skills Forecasts and Proposed Schedules of Work, which set out the emerging industry trends, skills needs and training priorities over a four year period. The aim of these cross sector projects is to develop training package components that address eight common skills areas across multiple industries in a coordinated and efficient way.

The Cyber Security Cross Sector Project, led by PwC's Skills for Australia, seeks to understand industry support for developing common Cyber Security units that can be contextualised across various industries. This project also aims to better understand what these units might look like, how they might be delivered, and what benefits or risks need to be considered with any potential changes to existing vocational training. This project complements much of the work that is already underway to improve Australia's Cyber Security and cyber resilience for the future, such as the Australian Government's Cyber Security Strategy[2].

The Cyber Security Project Reference Group (PRG), consisting of IRC members and/or subject matter experts, is responsible for the direction of this Cross Sector Project. They provide governance and make decisions based on the industry and stakeholder groups they represent. Members of the Cyber Security PRG are listed below.

Table 1. Cyber Security Project Reference Group members

Name	Location	Training Package	IRC Representation
Michael Magelakis	VIC	BSB Business Services	Business Services IRC
Katina Jones	SA	CHC Community Services	Community Sector and Development IRC
John Fleming	NSW	CPP Property Services	Property Services IRC
Peter Mousaferiadis	VIC	CUA Culture and Creative Arts	Culture and Related Industries IRC
Sarah Kauppinen	ACT	PSP Public Sector	Defence subject matter expert
Wayne Wilson	NSW	FNS Financial Services	Financial Services IRC
David Masters	ACT	ICT Information and Communication Technology	Information and Communications Technology IRC
Emma Broadbent	NSW	ICT Information and Communication Technology	Information and Communications Technology IRC
Heidi Loncar	WA	LGA Local Government	Local Government IRC
Mark Shannon	NSW	MAR Maritime	Maritime IRC
Bill Galvin	NSW	SIT Tourism, Travel and Hospitality	Travel, Tourism and Hospitality IRC
Russ Evans	QLD	TLI Transport and Logistics	Rail IRC
Stuart Johnston	ACT	UET Transmission, Distribution and Rail	Transmission, Distribution and Rail IRC

[1] Center for Strategic and International Studies, *Hacking the skills shortage* (Intel Security , 2016) <https://www.mcafee.com/au/>.

[2] Cyber Security Strategy - Department of the Prime Minister and Cabinet, Australian Government

Mark Harper	WA	AUR Automotive	Automotive Strategic IRC
Peter Blanshard	NSW	AUR Automotive	Automotive Strategic IRC

This document is a synthesis of findings from a literature review and stakeholder consultations conducted during August through to October 2017. The literature review includes a scan of domestic and international research focussing on emerging industry trends, skills needs and training priorities for Cyber Security. Stakeholder consultations include input from different stakeholder types (employers, industry associations, training providers, subject matter experts) from all States/Territories in Australia and from a range of industries. Insights from research and consultations will feed into a Case for Change document, which will present a concise, evidence-driven justification for potential changes to vocational training, the benefits and risks to be considered, and any implementation considerations. The Case for Change will be developed under the steer of the Cyber Security PRG, and is the ultimate deliverable due to be submitted to the AISC by end of November 2017.

For questions about this paper or the Cyber Security Cross Sector Project, please contact PwC's Skills for Australia at info@skillsforaustralia.com.

Executive Summary

In today's economy, the protection of digital assets is a key element in the long term competitiveness and survival of organisations. With cybercrime on the rise, there is a huge demand for Cyber Security professionals with industry aligned skills to identify, respond to and monitor Cyber related threats. Despite this demand, Cyber Security roles remain unfilled due to a lack of industry aligned Cyber Security skills. Employers are increasingly turning to formal and informal training for existing employees to help address skills gaps.

In order to better understand the challenges, issues and opportunities with vocational education and training in Cyber Security skills, PwC's Skills for Australia conducted a literature review and extensive stakeholder consultations from August through to October 2017. In total, we received input from 132 stakeholders across 27 different industries, and all states/territories. Key findings from our research and consultations are outlined below.

Current and future industry trends shaping the need for Cyber Security skills in the workplace

- There is a critical shortage of skilled Cyber Security professionals, both in Australia and overseas.
- The increased dependence on digital technology and digital connectivity, use of cloud based technologies and internet of things (IoT) data is driving increased demand for Cyber Security skills in the workplace.
- The rapid pace of digital and technological change, and rapid evolution of Cyber threats is exposing an increasing number of organisations to Cyber threats.

Cyber Security skills needs

- Overwhelmingly, we heard that there is a clear need for improved awareness and understanding of Cyber Security at every employee level in an organisation.
- A key skill set required by industry is the ability to detect and respond to Cyber threats or intrusions. Additional skills include identifying and securing potential vulnerabilities; assessing risks, hazards and vulnerabilities in a network or business environment; and implementing Cyber Security solutions to resist security attacks.

Effectiveness of existing vocational training

- Employers across a wide variety of industries are experiencing difficulty in finding workers with suitable Cyber Security skills.
- While some training packages do contain units related to Cyber Security skills, the content is not aligned with industry skills needs.
- Many employers are needing to invest time and money in training their employees in Cyber Security skills.

Benefits and risks of developing "common" Cyber Security units

- Benefits of implementing common units in Cyber Security include greater consistency in vocational training across industry sectors and a higher level of awareness of Cyber Security amongst workers.
- One risk is that the proposed new training products could quickly become outdated due to the rapid pace of technological change and relatively slower process of training product development and review cycles.
- Most stakeholders felt that the potential benefits of updating vocational education and training to include Cyber Security related skills far outweighs any potential risks.

Next steps

Since the establishment of the Cyber Security PRG in July 2017, we have presented a Case for Change report, which describes our evidence-based case for proposed changes to the VET system, including the potential development of new 'common' training products. This Case for Change will be shared with State and Territory Training Authorities (STAs) and endorsed by the Cyber Security PRG before submission to the AISC in November 2017.

Contents

1. Introduction

1.1 Purpose of the Cyber Security Cross Sector Project

The AISC has taken the opportunity to strategically address common skills needs identified in Industry Reference Committee (IRC) Industry Skills Forecasts and Proposed Schedules of Work through eight cross sector projects. The aim of these projects is to develop training package components that address those skills needs across industries in a coordinated and efficient way. The Cyber Security Cross Sector Project, led by PwC's Skills for Australia, is looking to understand industry support for developing common Cyber Security units to be used across multiple industry sectors. It is expected that the outcomes of this project will lead to a significant reduction in duplication across the national training system, making the system more efficient and easier to navigate for users. It is also expected that, in some cases, the development of common units and skill sets will assist individuals to move more easily between related occupations.

Key drivers of change

This project is proposed in response to the following drivers for change, identified in desktop research and stakeholder consultations:

1. **Shortage of adequately trained Cyber Security individuals in the Australian workforce**
   Over 85% of Australian IT professionals believe there is a critical shortage of Cyber Security skills. The same group of professionals believe that this will lead to 17% of Cyber Security roles remaining unfilled in the future. Furthermore, Australia has seen an increase in cyber attacks, which is likely to further increase the demand for qualified Cyber Security professionals.[3] Research shows that many organisations have difficulty recruiting Cyber Security trained employees.
2. **There are clear Cyber Security skills gaps in existing vocational training**
   Existing nationally endorsed training does not provide workers in all industries with the necessary Cyber Security skills and knowledge to succeed in the workforce. Stakeholders agree that there is difficulty finding workers with the appropriate Cyber Security skills.
3. **There is an opportunity for vocational training products to address these skill needs**
   The majority of survey respondents believe that current education and training equips learners "not at all well" with Cyber Security related skills. New common units provide an opportunity to increase Cyber Security awareness of workers at every level of an organisation.

1.2 Approach to the Cyber Security Cross Sector Project

1.2.1 Project methodology

Our approach to the Cyber Security Cross Sector Project is a combination of literature review and stakeholder consultations.

- **Literature review:** to understand current industry trends, skills needs and training priorities for Cyber Security. This involved a review of various Industry Skills Forecasts, analysis of existing units relevant to Cyber Security, and desktop research of domestic and international practice. Key findings from the literature review are provided in Section 2 of this report.
- **Extensive multi-channel approach to stakeholder consultations:** to get input from a diverse range of stakeholders (industries, geographic locations, stakeholder groups) through a variety of different channels, including one-on-one interviews, group discussions, an online nationwide survey, and webpage updates. Key findings from the stakeholder consultations are provided in Section 3 of this report.

To maximise the breadth and depth of our stakeholder reach, we leveraged our existing PRG and IRC member network, the broader PwC network, other Skills Service Organisations (SSOs) and Department contacts, training providers, subject matter experts and thought leaders. We also consulted with second degree contacts who were

[3] Southern Cross University, *Rising demand for IT professionals with cybersecurity skills* (2017) <https://online.scu.edu.au>.

referred to us through the course of this Cross Sector Project. There were four key channels by which stakeholders could contribute to this work:

- Interviews
- Nationwide industry survey
- Focus group discussions
- PwC's Skills for Australia webpage and social media channels (e.g. LinkedIn)

These are discussed further in Section 3 of this report.

1.2.2 Guiding principles for training product development

Our approach to the project has been guided by our principles for training product development, which determine that our work should be:

1. Industry-led;
2. Encourage broad and transparent stakeholder consultation;
3. Respond quickly to industry skills needs and priorities;
4. Be efficient and cost-effective; and
5. Produce high quality and independently validated training products.

We have also sought to align our objectives to meet the Council of Australian Governments (COAG) Industry Skills Council principles for reforms to Training Packages:[4]

1. Ensure obsolete and superfluous qualifications are removed from the system;
2. Ensure that more information about industry's expectations of training delivery is available to training providers to improve their delivery and to consumers to enable more informed course choices;
3. Ensure that the training system better supports individuals to move easily from one related occupation to another;
4. Improve the efficiency of the training system by creating units that can be owned and used by multiple industry sectors;
5. Foster greater recognition of skill sets; and
6. Ensures that new training courses can be developed as quickly as industry needs them and available to support niche skill needs.

1.2.3 Collaborating with industry and key stakeholders

The cross sector projects present an exciting opportunity for a more innovative approach to training package development. As the lead SSO, PwC's Skills for Australia is working collaboratively with industry and key stakeholders including other Skills Service Organisations and their IRC members, Commonwealth and State/Territory departments and government representatives, training providers and technical experts and researchers.

The Cyber Security PRG primarily comprises representatives from IRCs, who have nominated to represent their training package. The role of the PRG is to provide guidance and expertise throughout the training product development process and are the decision-making authority regarding potential training product development. PwC's Skills for Australia works closely with the Cyber Security PRG members to ensure that the views and opinions of industry are accurately reflected in the Case for Change report.

[4] *Communiqué for the COAG Industry and Skills Council Meetings Skills Ministers*, (Communiqué, 2015) <https://docs.education.gov.au/>.

2. Literature Review

2.1 Introduction

There is currently a skills shortage in Australia for Cyber Security trained professionals. As people increase their use of digital technology, and businesses rely more extensively on digital technology and equipment, Cyber Security skills are becoming a vital part of ensuring the growth of the Australian economy. It is expected that there will be an increased requirement for Cyber Security trained employees in the future.

The importance of Cyber Security skills is beginning to be more widely recognised across a broad range of organisations and industries. This section outlines the key findings from our literature review.

2.2 Summary of key findings

Employers report that Cyber Security skills are in short supply.

Employers in Australia are experiencing difficulty finding people with the required Cyber Security skills. For example, a 2016 survey commissioned by the Center for Strategic and International Studies found that 88% of Australian IT professionals believe that there is a domestic shortage of Cyber Security skills.[5] Furthermore, the increasing prevalence of cyber attacks and awareness of cyber issues is increasing demand for people with Cyber Security skills.[6]

Survey results from 200 UK IT security professionals suggest that encouraging young people and employees from non-IT backgrounds to train in Cyber Security is the most effective way to fill gaps in Cyber Security.[7] This survey also suggests that university degrees were not critical for training exceptional Cyber Security experts, instead suggesting that curiosity and on-the-job experience were the core skills required.

Cyber attacks pose an increasing threat to all organisations.

A number of security observers report cyber attacks to be increasing in sophistication and number. Organisations are becoming increasingly vulnerable as technology is used to augment an ever larger number of job roles and functions. Small organisations often believe that they are not likely targets, and avoid making serious investments in Cyber Security; however, research suggests that small businesses are in fact among the most likely targets for cyber attacks.[8]

With an increased reliance on the Internet of Things, industries are increasingly vulnerable to cyber attacks. These attacks can come in the form of targeted attacks or an indirect attack such as a Distributed Denial of Service attack. It is important that all organisations are up to date with the current trends in cyber attacks and that they are prepared to handle a possible disruption.[9]

A 2014 study showed that 99% of Cyber Security breaches that occurred in that year were caused by known vulnerabilities with known solutions.[10] This demonstrates the need for a higher level of Cyber Security awareness and training in all organisations in order to reduce the cost of breaches.

---

[5] Center for Strategic and International Studies, *Hacking the skills shortage* (Intel Security , 2016) <https://www.mcafee.com/>.
[6] Southern Cross University, *Rising demand for IT professionals with cybersecurity skills* (2017) <https://online.scu.edu.au>.
[7] MWR, *Survey finds new blood needed to fill cyber skills gap* (2017) <https://www.mwrinfosecurity.com/>.
[8] Nick Whigham, *Australian small business overlooked in government's Cyber Security push* (News.com.au, 2016) <http://www.news.com.au/>.
[9] Frost & Sullivan, *Cyber Security predictions for 2017: an asia-pacific perspective, according to Frost & Sullivan* (Cision, 2016) <http://www.prnewswire.com/>.
[10] Stephan W. Orfei and Sam Fancchini, *Cybersecurity and the hospitality industry* (Las Vegas Review Journal, 2016) <https://www.reviewjournal.com/>.

Basic awareness of cyber threats is critical, even for non-ICT employees.

Human error is the leading cause of security breaches, which is why it is critical for all employees to have basic Cyber Security knowledge.[11] As many organisation hold sensitive customer data, particularly organisations such as hospitals and local councils, security awareness training can help to secure everyone's data.[12]

When an organisation is compromised, it is often due to small errors, such as an employee opening a malicious attachment or leaving sensitive information unsecured.[13] As such, there is an ongoing need for employers to ensure all employees have a basic understanding of how to mitigate cyber threats, and how that might apply to their role in the organisation.

While organisations may believe that training all employees in basic Cyber Security habits is unnecessary, research shows that even the least effective of several anti-phishing training programs provided a seven fold return on investment, showing that training all employees in cybersecurity can be a valuable exercise for every organisation. Having all employees trained in Cyber Security awareness can lower an organisation's risk considerably.[14]

Some training packages already contain units related to Cyber Security

We conducted a broad initial search of unit titles on training.gov.au using the keywords "Information Technology", "cyber" and "security", and identified 193 units of competency.[15] We further filtered the Units of Competency to identify those specifically related to Cyber Security by using additional keywords including 'encryption', 'network security', 'risk', 'cloud' and 'vulnerability'; a total of 77 Units of Competency were identified. [16] Of these existing units related to Cyber Security, there was considerable overlap, duplication and redundancy. The final Case for Change will outline a proposal for reviewing existing units for AISC and (ultimately) IRC consideration.

[11] Rebecca Weintraub and Joram Borenstein, *11 things the health care sector must do to improve cybersecurity* (Harvard Business Review, 2017) <https://hbr.org/>.

[12] Lou Romero, 6 eye-opening findings about local government Cyber Security (PivotPoint Security , 2017) <https://www.pivotpointsecurity.com/>.

[13] Australian Information Security Association, *Cyber Security for senior executives* (2016) <https://www.aisa.org.au/>.

[14] Maria Korolov, *Does security awareness training even work?* (CSO, 2015) <https://www.csoonline.com/ >.

[15] Australian Government Department of Education and Training, See '*Nationally recognised training search portal*', (2017) <https://training.gov.au/Home/Tga>.

[16] At the time of writing of this Case for Change, the Department of Education and Training was working to develop and launch an algorithm to assist with content analysis of training package components. Depending on when this is made available, more sophisticated unit analysis may be possible and therefore may alter the number of potential units identified in this Case for Change.

3. Stakeholder Consultations

3.1 Consultation approach

3.1.1 Stakeholder engagement approach

A key objective of our stakeholder consultations was to achieve breadth of representation from industries, geographic locations, and stakeholder categories. To do this, we leveraged our existing PRG and IRC member network, the broader PwC network, other SSO and Department contacts, training providers, subject matter experts and thought leaders. We also consulted with second degree contacts who were referred to us through the course of this Cross Sector Project, pushing content through these networks and social media channels (LinkedIn, Twitter, industry newsletters, Skills for Australia website subscribers).

Figures 3, 4 and 5 in Appendix B shows the overall respondent profile (industry, geographic location and stakeholder category) of stakeholders consulted for the Cyber Security Cross Sector Project. In total, approximately 132 stakeholders have been consulted to date across our three main channels: interviews, survey respondents and focus group attendees.

- Top industries represented (out of a total 27 industries consulted):
    - Information and Communications Technology
    - Education
    - Business Services
    - Public Sector

- Top stakeholder categories represented:
    - Employers (including large and small-medium employers)
    - Training provider or other educational institution
    - Government Department
    - Technical experts

All states and territories had a voice in consultations.

3.1.2 Consultation channels

As mentioned in Section 1, there were multiple channels by which stakeholders could contribute to this project, and these are briefly noted below (key summary tables can be found in Appendix B). Each consultation followed seven lines of enquiry, also noted below.

Interviews

Interviews were held with key stakeholders over the phone or in person to better understand issues and opportunities. Pull and push methods were used to identify stakeholders for interviews: those who contacted us directly or via our networks (pull) and those who we targeted based on their industry representation, geographic location, or stakeholder category (push). Interviews were conducted from mid August to late October 2017. The interviewee profile is included in Appendix B.

Nationwide Industry Survey

A nationwide industry survey was developed to help reach a broader stakeholder group (beyond our own network), and to provide another channel for people to provide additional feedback. Again, push and pull methods were used to identify survey respondents; the survey was published via the PwC's Skills for Australia website and launched through our network and social media channels (LinkedIn, Twitter, industry newsletters, promoted at

industry conferences). The industry survey was live from 23 August 2017 to 25 October 2017 (9 weeks) and received 82 responses at survey close. The respondent profile is included in Appendix B.

Focus groups

Focus groups were offered as an additional mechanism for stakeholders to contribute their views and allow the opportunity for a mix of stakeholders to come together and engage in a dynamic, interactive group discussion about the lines of enquiry. The Cyber Security focus groups were held in Adelaide, Canberra, and Sydney.

3.1.3 Lines of enquiry

Six lines of enquiry were developed for the Cyber Security Cross Sector Project and used to guide our stakeholder consultations. These lines of enquiry were designed around what is known from existing research, skills or training that we want to test with stakeholders; and what gaps there are in existing research, skills or training that we need to know to prepare a Case for Change.

1. **Current and emerging industry trends:** What are the current and emerging trends in your industry – both domestically and internationally?
2. **Current and emerging skills needs:** What current and future Cyber Security skills are required of learners in your industry?
3. **Effectiveness of existing training:** How well does existing vocational education and training equip learners with the Cyber Security skills they need in industry? (Consider successful and unsuccessful elements of training, any existing gaps, keeping up with industry changes)
4. **Risks and benefits of change:** What are the risks and benefits of creating Cyber Security units that can be used across a large number of training packages?
5. **Training on different levels:** Are there certain Cyber Security skills needs for different levels in the workplace?
6. **Additional considerations:** What else needs to be considered that has not already been covered by these lines of enquiry? What elements of training delivery have been most successful that could be considered in delivering generic Cyber Security units?

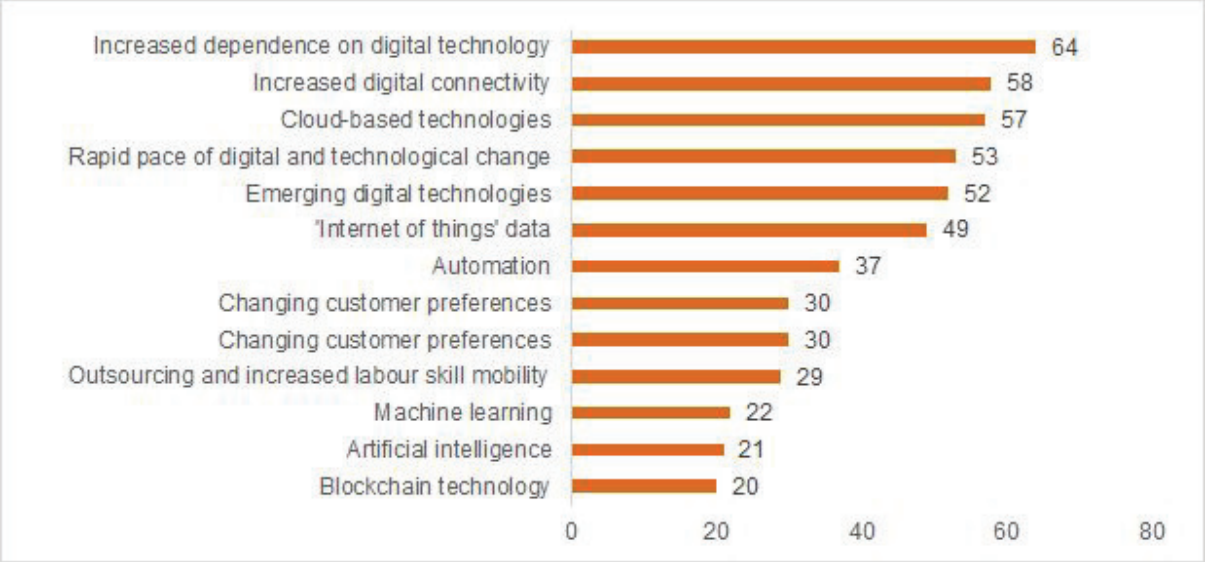
3.2 Current and emerging industry trends

In order for us to gain a better understanding of the industry trends, stakeholders were asked to identify which emerging trends in Cyber Security were most relevant to workers in their industry, and shaping the need for workers with Cyber Security skills.

The top industry trends related to Cyber Security include:

- Businesses are **increasing their dependence on digital technology**, opening their exposure to digital attacks and vulnerability. It is estimated that, in the future, more people will have a mobile phone than those who have electricity in their homes, making them a target for Cyber Security attacks, with small businesses being particularly vulnerable.
- **Cloud based technologies** exist on the internet and are a method of reducing IT infrastructure costs. The increase in utilisation of cloud technologies leads to increased vulnerability of information.
- **Increased digital connectivity** and the **internet of things data** continue to threaten privacy and pose risks to Cyber Security as the amount of data that is being collected and collated continues to expand. This data can include anything from GPS data to social media use and when this data is used collectively it can lead to privacy breaches.
- **Rapid pace of digital and technological change** - technology is progressing faster than ever and as a result it is becoming increasingly difficult to stay up to date with new and emerging technologies, and continually changing Cyber Security needs and skills.

Figure 1 *Number of survey respondents who selected each trend in response to "Which of these industry trends is driving demand for workers with Cyber Security skills in your organisation/industry?"*



Source: PwC's Skills for Australia, Cyber Security Cross Sector Project Industry Survey (base: 82 responses as of 25.10.2017)

3.3 Skills Needs in Cyber Security

In order to understand the specific Cyber Security skills needs required, we asked stakeholders to comment on the skills that are currently in high demand in their industry; and the future skills that will be needed for future workers in their industry. Stakeholders were also invited to comment on how difficult they found it to recruit employees with these specific skills.

Most highly demanded Cyber Security skills in industry:

- **Detecting and responding to threats or intrusions** - It is important that Cyber Security trained employees are able to detect threats or intrusions as soon as they occur so that they can be dealt with as soon as possible to ensure the least amount of disruption to an organisation.
- **Identifying and securing potential vulnerabilities** - Proactive detection of possible threats is a key skill required as it allows organisations to protect against potential threats before they occur.
- **Assessing risks, hazards and vulnerabilities in a network or business environment** - Cyber Security trained professionals need to be able to analyse an environment and identify the possible risks and provide solutions.
- **Implementing solutions that can deal robustly with potential security scares** - Cyber Security trained employees should be able to implement solutions that are able to resist security attacks.

62% of respondents had some trouble finding workers with relevant cyber security skills

New recruits are not meeting the demands of Cyber Security skills required in industry

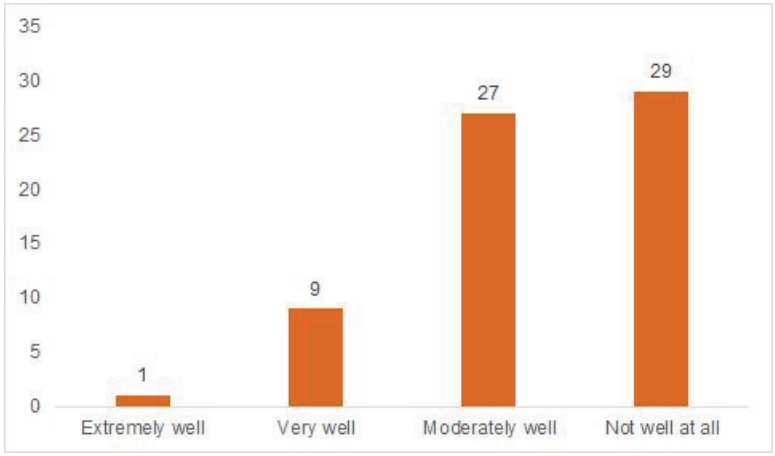
- 62% of survey respondents had some degree of difficulty finding workers with suitable Cyber Security skills. This feedback was also echoed in consultations, where many interviewees stated that there was a challenge in recruiting staff with the required skills.

- As one survey respondent commented, "There is a general lack of required base skills in Security in Australia."

3.4 Reviewing existing training

We asked our survey respondents to consider how well existing training equips learners with Cyber Security skills. As indicated in Figure 2 below, the majority of stakeholders believe that existing vocational training only equips learners "moderately well" or "not well at all" with the Cyber Security skills they need. Feedback from consultations similarly indicated that there are gaps in existing training.

Figure 2 *Survey statement: Overall, how well do you think existing vocational education and training equips learners with the Cyber Security skills they need in industry?*



Source: PwC's Skills for Australia, Cyber Security Cross Sector Project Industry Survey (base: 82 responses as of 25.10.2017)

Existing training for Cyber Security skills is failing to meet industry needs.

- There is a significant gap in the training of Cyber Security skills, resulting in many employers being unable to adequately fill available positions.
- One respondent commented on the high cost of current Cyber Security training at universities, believing that this restricts "accessibility and affordability resulting in perpetuation of skill shortage".

3.5 Risks and benefits of change

Throughout consultation, the majority of stakeholders were in support of the development of common Cyber Security units that could be contextualised across various industries. We also asked our stakeholders to comment on the potential impacts of change (including risks and benefits).

3.5.1 Potential risks of change

Obsolescence of new training products

Some stakeholders noted that there was a risk that the proposed new training products could quickly become outdated due to the rapid pace of technological change and the relatively slower process of training product development and review cycles. We have identified two methods to mitigate this risk. First, drafting units in a more generic nature that allows flexibility for training providers to refer to the most current examples and applications of Cyber Security related skills. Second, conducting more frequent reviews of Cyber Security related training products to ensure that training materials keep up with advancements in Cyber Security related

disciplines. Stakeholders were still in agreement that, despite this potential risk, the benefits of updating vocational training to include Cyber Security related skills far outweighs the negative prospects.

Consider funding arrangements and differences between state/territory jurisdictions

Differences in funding between state/territory jurisdictions was noted by stakeholders as a potential barrier to optimum uptake of a potential skill set. Nonetheless, a large part of the utility of s skill set is that they consist of units that could be imported into other training packages, helping to improve the potential flexibility of the VET system.

3.5.2 Potential benefits of change

Industry wide

- Organisations with a specialised cyber workforce will be able respond more effectively to sophisticated cyber attacks. If cyber skills are not improved, it could lead to an embarrassing data breach.[17]
- Reduced cyber risk in operational technology systems such as cars, traffic lights, mining systems.
- Increased security of ATM, credit card and mobile banking applications will foster trust in Australia's financial system.
- Confidence in the Cyber Security/digital technologies will open new business opportunities and boost future economic growth in Australia.

Industry/Employers

- Address current Cyber Security skills shortages.
- Improved alignment of training products to the needs of industry.
- Increased relevance of workers' skills to organisations.
- Increased efficiency in cyber operations.

Registered Training Organisations

- Increased flexibility in training product offerings.
- Potential for increased enrolments and completion rates.
- Improved efficiency of the training system through the removal of duplicate/obsolete units of competency and qualifications.

Learners

- Increased awareness of Cyber Security issues.
- Increase in individuals' ability to recognise and solve potential cyber problems before they become an issue for an organisation.
- Improved job opportunities for learners in Cyber Security.
- Increased contemporary skills and knowledge in Cyber Security.

3.5.3 Potential risks if no changes are made

Australia's economy will be left behind, impacting international competitiveness and threatening national security.

If no changes were made to vocational education and training in Cyber Security skills, there is a risk that more cyber threats will go unchecked. Stakeholders were of the view that a lack of change in this area could inhibit Australia's economic growth and stifle innovation, threatening Australia's international competitiveness.

[17] Cybersecurity skills gap widens, despite clear demand for experts (2017) <http://www.hrdive.com>

Increased financial cost to organisations

The financial cost of responding to cyber attacks retrospectively is significant. Stakeholders expressed serious concern that organisations would increasingly fall prey to cyber criminals due to low or inadequate Cyber Security awareness in their workforce.

Continuing shortage of Cyber Security talent

Stakeholders raised serious concerns about the continued shortage of Cyber Security talent in Australia if no steps are taken to improve Australia's vocational education and training. This was seen to have a potential dual impact: poor pipeline of future Cyber Security talent, and loss of existing talent to other countries.

Skills being taught in silos

Currently, employers are looking to other training options outside of the national VET system to train for the Cyber Security skills they need, specifically to their own software, procedures and technology. If industry and company agnostic training is not introduced, there is a risk that workers will possess siloed Cyber Security skills which make it more difficult to transfer across industries or companies.

3.6 Training on different levels

During consultations with stakeholders, it was proposed that Cyber Security units be specified to different levels of vocational education. Stakeholders suggested a basic introductory unit designed to meet the needs of most people working in organisations and a second more advanced series of units to target managerial or higher employees at an organisation. Throughout consultations, there was also broad support for the creation of a skill set in 'Cyber Threat Intrusion/Detection and Response' to allow for specialisation in Cyber Security skills. Additional advanced Cyber Security skills identified during stakeholder consultations include:

- **Cyber threat intrusion/detection and response skills**, to monitor network traffic, manage and respond to unusual or suspicious activity on the network to protect a business from cyber attacks.
- **Network and web application vulnerability assessment skills,** to identify security vulnerabilities on the network, web applications and produce recommendations to remediate identified security issues across existing infrastructure.
- **Cyber risk assessment skills**, to identify cyber risks and ultimately help to reduce Cyber Security incidents in organisations.
- **Managing and monitoring network access control skills,** to protect a network from internal or external Cyber Security threats and incidents by applying network security controls such as intrusion preventions systems, firewalls etc.
- **Cyber Security incident response skills**, to conduct cyber and forensic investigations such as computer memory analyses, network packet capture or malware analysis.
- **Secure software development skills,** to help guard against security vulnerabilities and data breaches in software or software code.

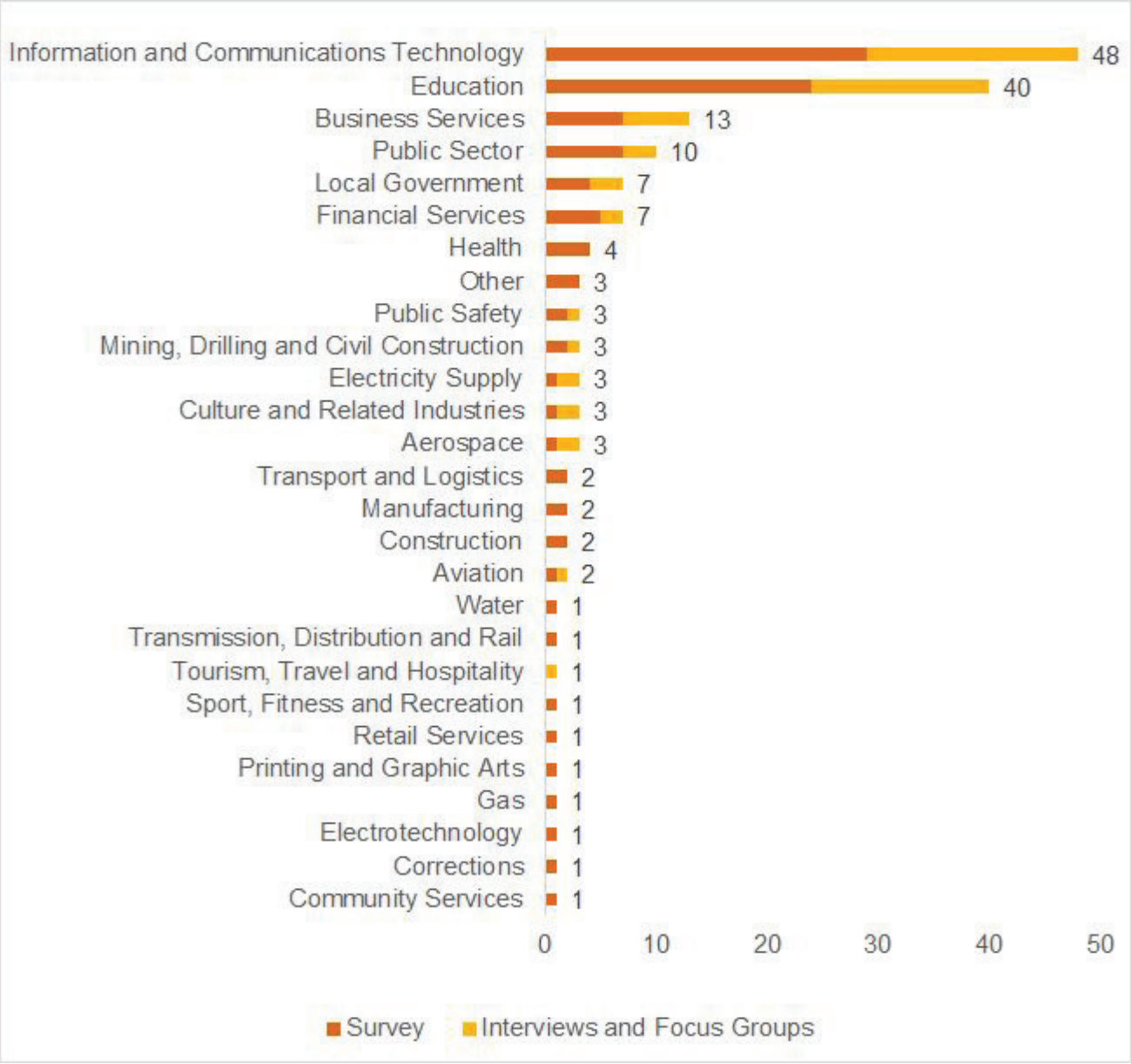
4. Appendices

Appendix A - Terminology

Acronym	Meaning	Definition
AISC	Australian Industry and Skills Committee	A body consisting of industry and peak body representatives, which advises Commonwealth and State Industry and Skills Ministers on the implementation of national vocational education and training policies, and approves nationally recognised training packages for implementation in the VET system.
AQF	Australian Qualifications Framework	A national framework for regulated qualifications in the Australian education and training system, which sets forth principles to ensure consistency in the format of qualifications.
COAG	Council of Australian Governments	An organisation consisting of the federal government, state/territory governments, and Australian Local Government Association.
IRC	Industry Reference Committee	Committee comprised of subject matter experts, employers, industry association representatives in their respective industry, which have been appointed by the AISC and have decision making authority over their training package.
PRG	Project Reference Group	A group holding decision making power for a cross sector project, comprised of IRC members and subject matter experts.
RTO	Registered Training Organisation	An organisation registered to deliver accredited vocational training.
SSO	Skills Service Organisation	Independent service organisations that support Industry Reference Committees (IRCs) in their work developing and reviewing training packages.
UoC	Unit of Competency	The specification of knowledge and skill, and the application of that knowledge and skill, to the standard of performance expected in the workplace. A unit of competency is the smallest unit that can be assessed and recognised.

Appendix B - Stakeholder consultations

Figure 3 *Respondent profile from stakeholder consultations by industry (across all channels: interviews, surveys and focus groups).*

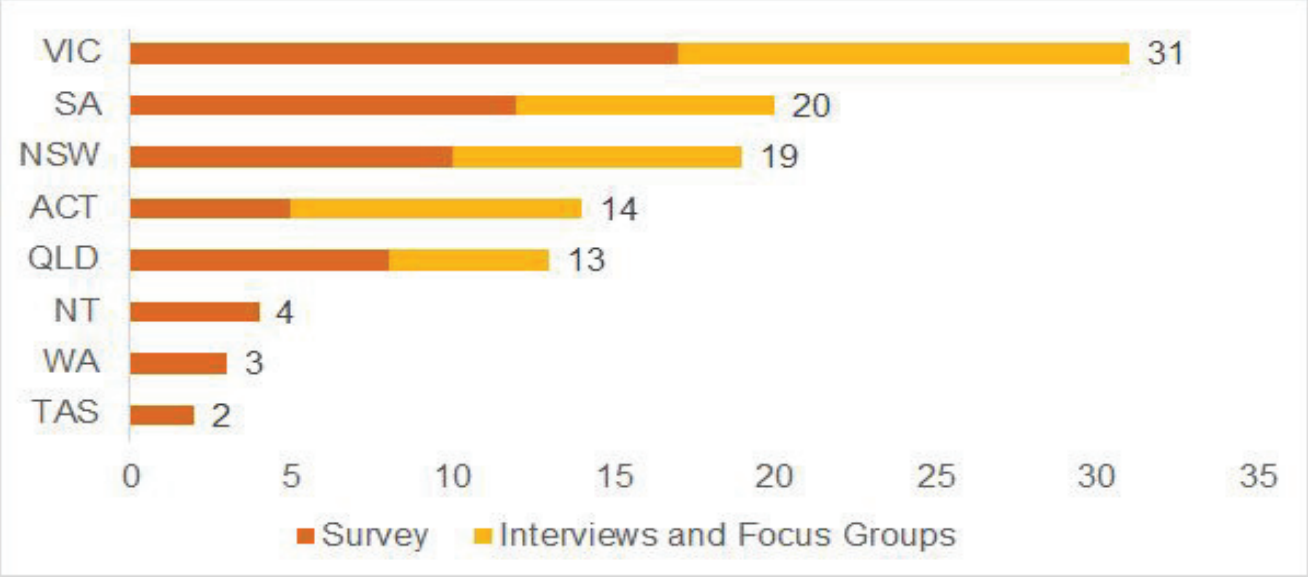


Source: PwC's Skills for Australia, Cyber Security Cross Sector Project Industry Survey, Interviews and Focus Groups (base 132 responses as of 25.10.2017). Respondents were invited to nominate up to two industries.

Figure 4 *Respondent profile from stakeholder consultations by stakeholder type (across all channels: interviews, surveys and focus groups).*

Source: PwC's Skills for Australia, Cyber Security Cross Sector Project Industry Survey, Interviews and Focus Groups (base 132 responses as of 25.10.2017). Respondents were invited to nominate up to two stakeholder types.

Figure 5 *Respondent profile from stakeholder consultations by state/territory (across all channels: interviews, surveys and focus groups).*



Source: PwC's Skills for Australia, Cyber Security Cross Sector Project Industry Survey, Interviews and Focus Groups (base 132 responses as of 25.10.2017). Respondents were invited to nominate up to two stakeholder types.