Cyber Security

A Roadmap to enable growth opportunities for Australia

2018

CSIRO FUTURES

CSIRO Futures is the strategic advisory arm of Australia's national science agency.

www.csiro.au

CSIRO

AustCyber
Australian Cyber Security Growth Network

AUSTCYBER

The Australian Cyber Security Growth Network (AustCyber) is the industry-led Cyber Security Growth Centre, one of the centres under the Australian Government's Industry Growth Centres Initiative. AustCyber is working with organisations across the economy to ensure that Australia is a global industry leader, and is able to export cyber security solutions in the growing global marketplace while helping Australian organisations of all sizes and across all sectors to be more resilient to the growing threat of malicious cyber activity.

CSIRO FUTURES

CSIRO Futures is the strategic advisory arm of Australia's national science agency. We work with senior decision makers in Australia's largest companies and government to help them translate science into strategy and plan for an uncertain future. We build on CSIRO's deep research expertise to help our clients create sustainable growth and competitive advantage by harnessing science, technology and innovation.

DATA61

CSIRO's Data61 is addressing the challenge of how to create Australia's data-driven future with science and technology, by partnering with industry, government and universities globally to deliver economic, societal and environment outcomes. As Australia's largest digital innovation network, Data61's capabilities range from cyber security, confidential computing, IoT, robotics, machine learning and analytics, software and programming to behavioural sciences and more.

CSIRO acknowledges the Traditional Owners of the lands that we live and work on across Australia and pays its respect to Elders past and present. CSIRO recognises that Aboriginal and Torres Strait Islander peoples have made, and will continue to make, extraordinary contributions to Australian life including in cultural, economic and scientific domains.

Foreword

Rapid global disruption and disintermediation is creating new industries and dramatically transforming old ones. As traditional boundaries collapse, Australia has a strategic national advantage in the critical cyber security space. Growing a strong and competitive Australian cyber security sector will not only underpin the future evolution of every Australian industry as it embraces digital opportunities, but forge a new economic pillar of its own. But our national advantage will only materialise through deep collaboration to fuel continued growth of the Australian economy – we need a common vision.

This Cyber Security Industry Roadmap brings together the expertise and networks of CSIRO and AustCyber, the Australian Cyber Security Growth Network, to recognise that common vision and map out the road to success for our cyber security sector. We apply world-class scientific and technological expertise to steer business, government and society through the challenges we must navigate over the next 10 to 15 years, deflecting the threats and seizing the opportunities presented. For example, Australians are already starting to benefit from an emerging industry focused on collection and use of genomic and health data, which is both improving the nation's health and providing jobs and economic growth. As we integrate data and digital technologies into everything we do, its integrity and security will be key to our healthy future.

We have an opportunity to be a world leader in this field. We can build this industry with skills from our world-class education system, testbeds supported by our small but sophisticated market, and alignment with cultures and time zones in our geographic region. The concentration of some of the world's brightest minds, in a thriving economy, working in shared languages and business hours through the Indo-Pacific is an incredible advantage.

As Australia responds to major global disruption, a strong local cyber security sector will not just enable our economy to grow and compete, but create an opportunity to excel on the world stage. It will take collaboration, coordination and commitment to deliver, and this Roadmap sets out the clear steps along the path to achieving this bold vision for Australia's future prosperity.

At CSIRO, we are focused on the excellent science that drives breakthrough innovation, and gives our businesses and industries the edge in an increasingly competitive global marketplace. Though the integration of our Data61 business unit across the depth and breadth of CSIRO, we're creating Australia's data-driven future and leading the digital change. We work closely with industry and the Australian Industry Growth Centres to align our science with your needs.

Larry Marshall
CSIRO Chief Executive

At AustCyber, we are working with organisations across the economy—public, private and research sectors alike—to ensure that Australia is a global industry leader, able to export cyber security solutions in the growing global marketplace while helping Australian organisations of all sizes and across all sectors to be more resilient to the growing threat of malicious cyber activity.

Michelle Price
AustCyber Chief Executive Officer

Executive Summary

Cyber security – vital for future industry growth

Cyber security has never been more important, both as an enabler for Australian industry and as a source of economic growth itself.

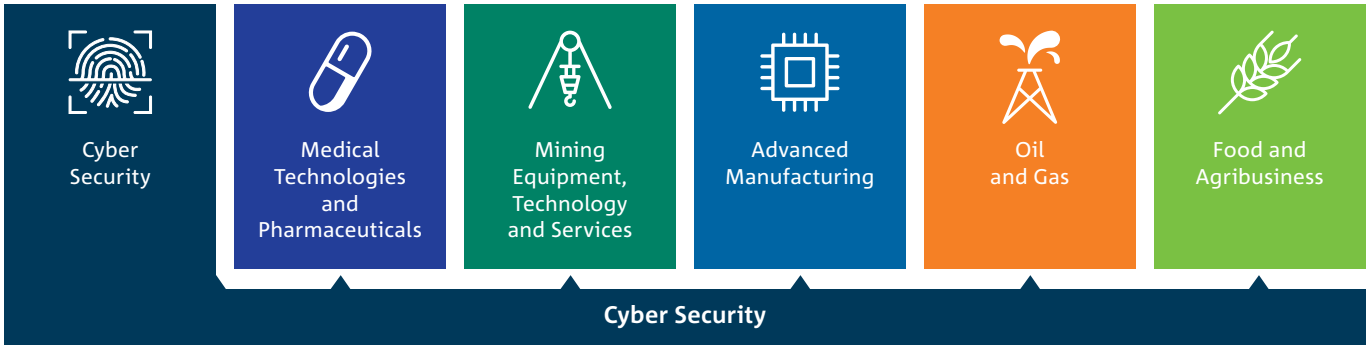
Vision for Australia's Cyber Security Sector

A globally competitive Australian cyber security sector that enables Australian organisations to pursue digitally driven growth, and supports greater trust and confidence to participate in the international economy.

As an enabler for industry, cyber security's importance is being driven by the global business environment becoming increasingly interconnected and reliant on data and digital technologies. As a result, organisations need to think of cyber security not just in terms of compliance and risk mitigation, but as an essential business function that is fully embedded in processes and systems.

And as a source of economic growth itself, Australia's burgeoning cyber security industry has a unique opportunity to deliver services and solutions in a globally-competitive, export-facing industry.

This Roadmap primarily focuses on the first aspect: the role cyber security (as a horizontal sector) can play in enabling growth opportunities in other sectors. In particular, the report concentrates on the priority Australian sectors aligned with Australian Government's Industry Growth Centres initiative.



At present, Australia's cyber security sector is small; however, it is forecast to triple its revenue over the coming decade due to increased demand for cyber security products and services.

The majority of Australian organisations currently lack the capacity to employ large internal cyber security teams which, in turn, creates demand for external, often international cyber services.

AustCyber's Cyber Security Sector Competitiveness Plan – a companion to this Roadmap – provides details about the cyber security industry and skills requirements that will allow the Australian sector to capture value from this increased demand.

$2.2 billion
2016 revenue

$6.0 billion
2026 revenue

10 year CAGR 10.6%

19,500
2017 cyber security workforce

31,600
2026 cyber security workforce

Digital trends transforming industry

Digital transformation is providing numerous Australian industries with unparalleled opportunities for value creation.

These trends illustrate that digital technologies, connectivity and automation are having a profound impact on the way organisations operate. These trends are not discrete, and exert an influence on an evolving cyber security threat landscape, with diverse and unanticipated cyber security risks now affecting businesses, governments, and people.

Each trend creates cyber security implications for Australia's industries, and will create opportunities for Australia's cyber security sector.

INCREASED DATA EXCHANGE

The volume of data generated and exchanged between equipment, people and businesses is leading to meaningful insights that support disruptive business models and technologies.

ENHANCED EXPERIENCES

Digital technologies are allowing people to have increasingly personalised and enhanced experiences, which is leading to changes in human expectations and behaviours.

GLOBALLY CONNECTED

Global connection through the digital world is enabling trade, empowering people with access to information and novel products and services; and allowing seamless communication for improved social connections.

TRANSFORMED SUPPLY CHAINS

Digital technologies are transforming supply chains, creating greater transparency, increasing efficiencies and blurring traditional boundaries.

Delivering a cyber secure future

Australia's small but well-developed market provides an exemplary testing ground for pilot programs to then be rolled out in larger economies.

Three themes have been developed via diverse industry consultation to understand how cyber security solutions can lead to more effective organisation and business operations, and improve Australia's overall cyber security posture to take advantage of digital transformation. Industry can engage immediately, in the short and medium terms in these themes, which are: (1) trusted ecosystem, (2) secure by design, and (3) robust and resilient. The themes cut across sectors, and discuss how Australia can embed cyber secure behaviour by building trust, improving design processes and raising overall cyber-resilience.

These themes build on the goals established by AustCyber to: (1) grow an Australian cyber security ecosystem, (2) export Australia's cyber security to the world and (3) make Australia the leading centre for cyber education.

As cyber security solutions move from being a post-development consideration to a design-phase consideration that is tightly integrated with the industry vertical, time to market will improve, as will the reputation of the products and services being developed in Australia.

Trusted ecosystem

Creating digital ecosystems that are highly trustworthy, allowing for rapid exchange of information and providing a stronger environment for trade.

Trusted partners
User-friendly and trusted sharing of information within supply chains, with third parties and with customers.

Threat intelligence sharing
Information about credible cyber security threats is shared within industry efficiently, allowing credible threats and risks to be quickly understood.

Collaborative demonstration projects
Demonstration projects illustrate how a trusted ecosystem may be established to create commercial value within Australia's priority growth sectors.

Resources and guidelines
Best-practice guidelines and tailored cyber security assessment resources are available, customised to Australia's various industries and adaptable to the unique circumstances of businesses.

Onshore capability
The judicious procurement of locally developed cyber security solutions is encouraged where available, helping to maintain a critical mass of onshore cyber capabilities.

Secure by design

Ensuring new products, services, platforms and processes are designed with cyber security as a key consideration.

Assurance of secure products
Guidelines establish a baseline for built-in cyber security in products and services that harmonises with international standards, allowing for improved exportability.

Secure by design skills in workplaces
Cyber security workplace skills are strong. Companies involved in the development and commercialisation of new technologies embed strong cyber security early in the design process.

Security embedded in ICT training
The gap between cyber security and ICT education is bridged by embedding more cyber security aspects into all tertiary information technology courses.

Research and industry collaboration
Australia's cyber security sector and the research community collaborate to help Australian industry underpin innovation with strong cyber security.

Secure trade and supply chains
Contractual negotiations and trade agreements clearly integrate cyber security measures in the development phase, leading to much greater security across supply chains.

Robust and resilient

Building greater cyber maturity and resilience in Australian industry and communities by developing a robust security culture.

Awareness in the community
Community awareness about the importance of cyber security is strong, supported by a targeted, high-profile education campaign.

Workforce skills
Awareness of cyber security basics in the context of workplaces is strong throughout all levels of staff, with companies adopting appropriate risk based practices.

Frameworks for cyber security
New frameworks and improved governance enables more innovation, while ensuring cyber resilience is prioritised.

Strong leadership
Executive and Board level cyber security literacy and education initiatives are supported and well attended, leading to improved cyber security awareness within company leadership structures.

Australia's reputation
Australia's cyber security sector in collaboration with the priority sectors have built a national reputation for cyber security excellence across key cyber security pillars, leveraging strengths of the research community.

Universal cyber care
Technology solutions focused on helping to raise the general cyber security hygiene of the Australian public and businesses have been investigated and developed.

Actions for cyber secure growth

Realising the themes requires change via collaborative action, with the Australian cyber community working closely with businesses, research institutes, governments, industry associations and the Industry Growth Centres. Presented over immediate to medium-term timeframes, each action is aligned to one or more of the themes. Many of the immediate actions are already in process in cyber literate sectors such as finance and defence; however, further consideration is required in order for them to be implemented across broader Australian industry.

	IMMEDIATE
Guidelines and frameworks	Improve guidelines for best practice cyber security hygiene
Threat intelligence sharing	Improve shared threat intelligence
Skills and training	Improve basic cyber security practices Improve cyber literacy in company leadership
Cyber security awareness	Develop business awareness and cyber resources Build community awareness Celebrate home grown cyber solutions
Collaboration with Australia's growth industries	Establish demonstration projects
Improved cyber-physical systems	Develop solutions for areas of poor connectivity

For detailed information on actions, please see chapter 3.

Trusted ecosystem | Secure by design | Robust and resilient

SHORT TERM (1-3 YEARS)	MEDIUM TERM (3 – 5 YEARS)
Develop data sharing frameworks	Develop agile frameworks for technology adoption
Improve baseline device and platform security	Improve frameworks for international trade
	Improve global threat intelligence sharing
Build 'secure by design' workforce skills	Embed cyber skills into general workforce development
Embed cyber skills into ICT workforce	Create active education experiences
Improve communication of secure by design features →	
Build solutions for Australia's growth industries	Build Australian exports and global reputation
Transform business models	Ensure cyber security is considered in trade negotiations
Mitigate legacy systems risk	Establish trusted inter-site networks
Improve data collection	

Cyber security for Australian industry

To be truly effective, Australian industry and the cyber community must tailor the enabling themes and actions to each industry's specific opportunities for growth, such as the examples given in the diagram below.

By unpacking growth opportunities presented within the themes in this report, Australian industry and the cyber security sector can both work towards the development of competitive offerings for local and international markets.

For Australia to be globally competitive, cyber security must underpin the data-driven transition of every sector in the economy.

Medical Technologies and Pharmaceuticals (MTP)

Opportunity for growth	Company value creation	Cyber security challenges
Diagnostic products and services Novel business and service models around the collection, interrogation, interpretation and packaging of medical and population data.	• New business opportunities • Shortened R&D cycles • Better patient insights • Precision products with higher demand/profit • Novel clinical trial models	• Data sharing • Data privacy and ownership • Data integrity • Insider threats • Theft and extortion

Priority actions

Secure by design	1. Improve healthcare networks and infrastructure
Trusted ecosystem	2. Develop frameworks for improved clinical data sharing

Mining Equipment, Technology and Services (METS)

Opportunity for growth	Company value creation	Cyber security challenges
Data driven mining decisions Using data throughout the mining lifecycle to optimise mining operations, reduce timeframes for making high value decisions and optimise response to market demands.	• Trusted insider access to data • New business model opportunities • Trusted engagement with mining companies	• Operational technology (OT) • Connected equipment and sensors • Availability of data • Anomaly detection • Volatility of markets

Priority actions

Secure by design	1. Improve the security across connected mining environment
Trusted ecosystem	2. Improve the safe integration of legacy technologies and systems

Advanced manufacturing

Opportunity for growth	Company value creation	Cyber security challenges
Customised high margin solutions Develop manufacturing services that integrate suppliers and customers to provide customised products that can generate higher margins.	• Customer willingness to pay • Greater loyalty • Novel processes and products • Collection of more data • Greater potential for range expansion	• Security confidence • Insider threats • Supply chain integrity • Data integrity • Data availability • Connected equipment

Priority actions

Trusted ecosystem	1. Improve channels for supply chain data sharing
Secure by design	2. Ensure secure integration of cyber-physical manufacturing systems

Oil and gas

Opportunity for growth	Company value creation	Cyber security challenges
Digital operations and maintenance Transform operations and maintenance activities across onshore and offshore developments through integration and adoption of digital technologies.	• Improved workforce safety • Improved productivity and cost efficiencies • Predictive maintenance eliminates down-time	• Legacy assets • Control and availability of OT • Security of networks • Physical security • Data sharing • Intelligence sharing • Data integrity

Priority actions

Trusted ecosystem	1. Improve national and global intelligence sharing
Robust and resilient	2. Implement active education programs

Food and agribusiness

Opportunity for growth	Company value creation	Cyber security challenges
Premium interactions Export products that generate a premium price due to their quality and novel attributes, underpinned by the ability to provide accurate reporting on provenance.	• Preserve premium prices • Reduced food fraud • Trust based competitive advantage • Potential for service and value-add	• Digital maturity • Security of sensors • Data sharing • Availability and authentication of provenance data • Food supply chain security

Priority actions

Trusted ecosystem	1. Build awareness of cyber solutions
Robust and resilient	2. Improve collaborative data sharing

Contents


/Administration
/Human Resources
/Legal
/Accounting
/Finance
/Marketing
/Publicity
/Promotion
/Research
/Business
/Development
/Engineering
/Manufacturing
/Planning

Cyber security: enabling industry growth

1 Cyber security: enabling industry growth

Vision for Australia's Cyber Security Sector

A globally competitive Australian cyber security sector that enables Australian organisations to pursue digitally driven growth, and supports greater trust and confidence to participate in the international economy.

Cyber security has never been more important, both as an enabler for Australian industry and as a source of economic growth itself. The global spend on cyber security is projected to increase by 88% by 2026,[1] driven by the movement towards digitisation, with data, digital technologies and infrastructure, and connectivity being critical to almost every industry. Australia's burgeoning cyber security industry has a unique opportunity to deliver services and solutions in a globally-competitive, export-facing industry.

To take full advantage of this industrial transformation and remain globally competitive, Australian industry must shift its perceptions on cyber security from a risk and compliance-based requirement to an essential business function that is fully embedded in processes and systems. This concept is the central focus of this report. Furthermore, building cyber-resilience in Australian industry will support the economy to become a trusted place in which to do business in a highly-competitive global trade environment. Australia is well positioned to pursue digitally-driven opportunities, for example:

- Genome sequencing technology and advanced analytics will allow for the development of an industry that uses genomic data to develop precision medical products and services, underpinned by advancements in clinical networks.
- Advances in robotics and autonomous systems are allowing oil and gas businesses to remove workers from dangerous working environments by engaging in digital operations and maintenance.
- Industry 4.0 – the trend towards automation, machine-to-machine and human-to-machine communication and artificial intelligence (AI)[2] – is enabling an industrial transformation towards fast, flexible, high-quality and efficient manufacturing.

These opportunities are underpinned by technologies that present new challenges, expose social and technological vulnerabilities, and therefore have important implications for cyber safety. A technological example is the Meltdown and Spectre computer vulnerabilities (disclosed in January 2018) that exploit critical vulnerabilities in modern ICT processors and have an impact on most organisations. These vulnerabilities allow software to steal data (which might include passwords, personal information and business-critical documents) which is processed on the computer.[3]

As data and digital systems become increasingly important to Australian organisations, so too does the need to protect the value they create. This is where Australia's cyber security sector will play a vital role in the future prosperity of Australian industry.

1 Australian Cyber Security Growth Network Ltd (2018). *Australia's Cyber Security Sector Competitiveness Plan - 2018 Update*.
2 Department of Industry, Innovation and Science (n.d.). *Industry 4.0*, [Online] Available from: https://industry.gov.au/industry/Industry-4-0/Pages/default.aspx Accessed: 27/02/2018
3 Graz University of Technology (2018). *Meltdown and Spectre*, [Online] Available from: https://spectreattack.com/ Accessed: 27/02/2018

1.1 About this report

> "By developing products and services that address the specific cyber security needs of these sectors, Australian companies can develop distinctive, competitive offerings for the global marketplace."
>
> AustCyber[4]

This Roadmap is focused on the role cyber security (as a horizontal sector) can play in enabling growth opportunities in other sectors. In particular, the report focuses on the cyber security's role across five priority Australian sectors aligned with the Industry Growth Centre initiative (Figure 1).[5] In order to connect the rapidly evolving cyber security sector and Australia's priority growth sectors, this Roadmap leverages CSIRO's published Industry Roadmap series and AustCyber's Cyber Security Sector Competitiveness Plan (SCP – a companion report).

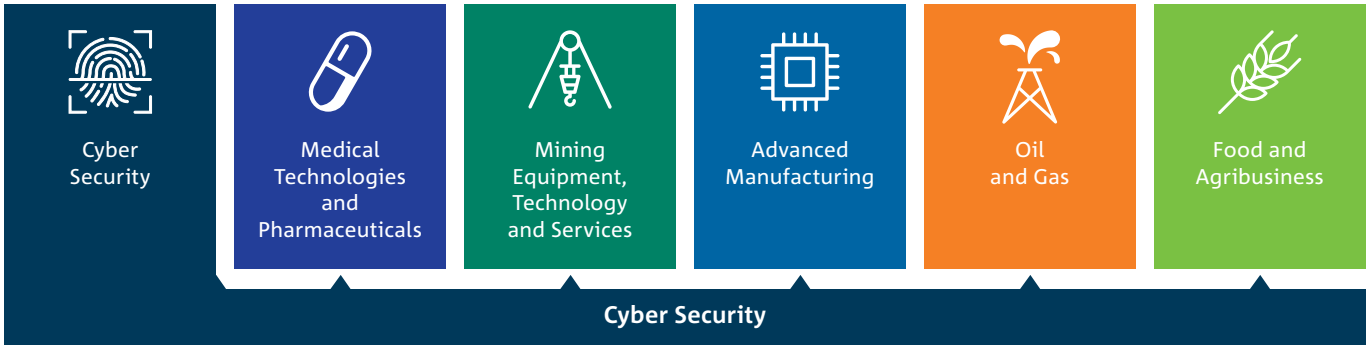
This Roadmap aims to:

- identify how stakeholders within the five priority sectors can better understand and leverage cyber security for growth
- allow cyber security organisations to understand sector needs and develop competitive and exportable offerings.

It will achieve this by:

- presenting growth-enabling themes and actions based on industry consultations that position cyber security as a growth-enabling business activity
- developing a framework that can be applied to the five sectors, and then be translated for rapid assessment across any sector within Australia's economy
- providing examples of how the framework can be applied to high-growth opportunities across the five identified priority sectors.

FIGURE 1: AUSTRALIA'S STRATEGIC PRIORITY GROWTH SECTORS



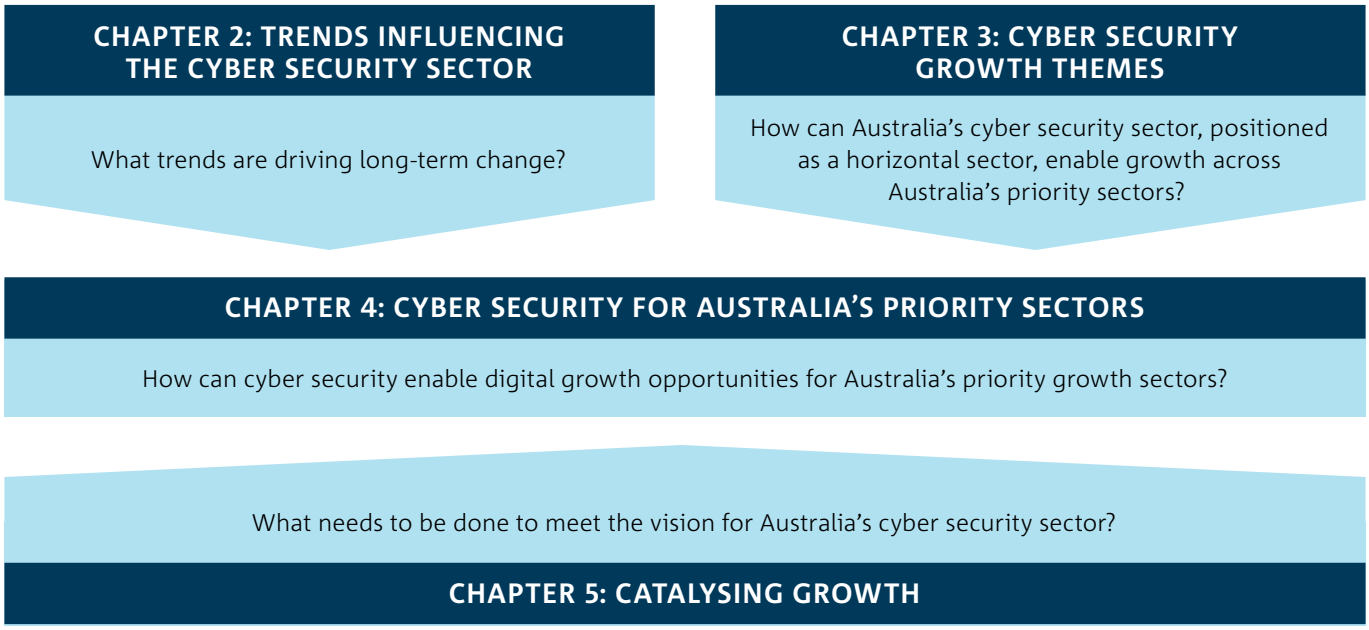
4 Australian Cyber Security Growth Network Ltd (2017). *Cyber Security Sector Competitiveness Plan*.

5 Department of Industry, Innovation and Science (n.d.). *Industry Growth centres,* [Online] Available from: https://industry.gov.au/industry/Industry-Growth-Centres/Pages/default.aspx Accessed: 27/02/2018

What is the difference between digitisation and digitalisation?

- **Digitisation** is the process of converting and representing an analogue source in a digital format – for example, converting a photograph to a jpeg file.
- **Digitalisation** is the application of digital technologies that alter the way individuals or businesses operate by providing new ways to increase productivity and revenue.

FIGURE 2: CYBER SECURITY ROADMAP STRUCTURE



Trends influencing the cyber security sector

2 Trends influencing the cyber security sector

Digital transformation is providing Australian industries with unparalleled opportunities for value creation.

The majority of Australian organisations currently lack the capacity to employ large internal cyber security teams, which creates demand for external, often international cyber services.

Globally, the cyber security sector was estimated to be worth around US$131 billion in 2017 (see Appendix 1). Australia's cyber security sector is relatively small, with revenues of around AU$2.2 billion in 2016. However, growth to meet local and international demand could see this revenue triple over the next decade (see Appendix 2).[6]

If the Australian cyber security sector intends to grow to meet increased demand, it is important that organisations understand and build on Australia's advantages and are aware of the challenges that must be overcome (see Appendix 3). One of Australia's key advantages is its excellent research quality, exemplified by its many dedicated research institutions, including Data61 – the nation's largest data innovation group. AustCyber's SCP provides detail on the cyber security industry and skills requirements that will allow the Australian sector to capture value from increased demand.

$2.2 billion
2016 revenue

$6.0 billion
2026 revenue

10 year CAGR 10.6%

19,500
2017 cyber security workforce

31,600
2026 cyber security workforce

CSIRO'S DATA61

Data61 is Australia's leading data innovation group, engaging in research and development to help drive Australia's data-driven future – a future where technologies for data will play a positive role for the society at large. Data61's science vision is motivated by the challenges and opportunities that are arising from digital technologies, focusing on two key dimensions:

1. Data you can trust – ensuring users can trust in the source of the data, the reliability of its conclusions, and trust that it will not be used to harm people

2. Technology that works for you – focused on how to build trustworthy data technologies that do what they are supposed to do, and nothing else.[7]

Data61's cyber security research focuses on: building trustworthy and resilient systems; understanding risk and building shared awareness; and strengthening the human and social dimension of cyber security.[8]

6 Australian Cyber Security Growth Network Ltd (2018). *Australia's Cyber Security Sector Competitiveness Plan - 2018 Update*.
7 Data61 (2016). *Our science vision*, [Online] Available from: https://data61.csiro.au/en/Who-we-are/Our-Science-Vision Accessed: 16/03/2018
8 Data61 (2018). *Cybersecurity at CSIRO's Data61*, [Online] Available from: https://www.data61.csiro.au/en/Our-Work/CyberSecurity-At-Data61 Accessed: 16/03/2018

2.1 Global digital trends

Effective strategy for any sector requires an understanding of the global trends that are affecting that sector.[9] CSIRO's Industry Roadmap series each identify global megatrends that will have an impact on the future growth of their respective sectors. These trends have been distilled into the four global digital trends that are driving business and consumer use of digital technologies, as highlighted in Figure 3.

These trends are not discrete, and illustrate the fact that digital technologies, connectivity and automation are having a profound impact on the way each sector operates. These trends influence and shape an evolving cyber security threat landscape, with diverse and unanticipated cyber security risks affecting businesses, governments and people. Australian organisations need to be proactive in their understanding of the implications associated with these trends, and agile in their response to the cyber security threats and opportunities that will emerge.

Each trend creates cyber security implications for Australia's industries, and will create opportunities for Australia's cyber security sector.

What is a cyber-physical system?

Cyber-Physical Systems demonstrate the convergence of objects in the physical environment with computing and communication capabilities. These engineered systems support the monitoring, coordination and control of physical systems, and will transform the way humans interact with the physical world. Because of their interaction with the physical world, these systems must operate dependably, securely and in real time.[10]

For example, manufacturing industries are increasingly adopting 'Industry 4.0' which involves cyber-physical systems: intelligent, self-regulating, automated manufacturing processes and machines that are capable of monitoring one another and making decentralised decisions about production and maintenance.[11]

FIGURE 3: DIGITAL TRENDS

INCREASED DATA EXCHANGE

The volume of data generated and exchanged between equipment, people and businesses is leading to meaningful insights that support disruptive business models and technologies.

GLOBALLY CONNECTED

Global connection through the digital world is enabling trade, empowering people with access to information and novel products and services; and allowing seamless communication for improved social connections.

ENHANCED EXPERIENCES

Digital technologies are allowing people to have increasingly personalised and enhanced experiences, which is leading to changes in human expectations and behaviours.

TRANSFORMED SUPPLY CHAINS

Digital technologies are transforming supply chains, creating greater transparency, increasing efficiencies and blurring traditional boundaries.

9 CSIRO Futures (2016). *Australia 2030: navigating our uncertain future,* Canberra.

10 Rajkumar, R., Lee, I., Sha, L., Stankovic, J. (2010). *Cyber-physical systems: the next computing revolution,* In Proceedings of the 47th Design Automation Conference (DAC '10). ACM, New York, NY, USA, 731—736.

11 Gallagher, S. (2017). *Industry 4.0 Testlabs in Australia – Preparing for the Future,* Swinburne University of Technology, Prime Minister's Industry 4.0 Taskforce.

2.1.1 INCREASED DATA EXCHANGE

The volume of data generated and exchanged between equipment, people and businesses is leading to meaningful insights that support disruptive business models and technologies.

Globally, the volume of data generated doubles every three years,[12] driven by increased digitisation and digitalisation across industries, governments and households. The ability to access and transform this data into meaningful insights will support advances and disruptions to business models, leading to increased industry productivity and, in some cases, improved quality of life. For example, in Australia, the Data Integration Partnership for Australia (DIPA) is just one initiative aimed at maximising the value of government data by combining datasets to gain a more complete and informed picture, creating new insights into important and complex policy questions.[13]

The volume, velocity, variety and veracity of data (the so called 'Four V's of Big Data') being generated and exchanged will create challenges to the data's utility. The variety of data – structured and un-structured – can make extracting actionable intelligence more difficult, such as unstructured social media content and semi-structured medical records.[14] Velocity of data creation presents challenges, such as managing real-time and high speed data creation. Its veracity (i.e. the confidence or trust in data) presents problems for decision makers, who need to be able to trust the data in order to use it. While these components of data exchange present challenges, once they are overcome, data inevitably creates value.

Increasing creation and utility of data affects cyber-physical systems, with insights gathered from data directly causing changes in the physical world. Industry examples of value creation through increased data exchange include the mining industry, where connected sensors on equipment, processes and people help to embed data driven mining decisions for improved operations.[15] In healthcare, data collected from patients and across the system is enabling new diagnostic platforms.[16]

Cyber security implications

Rapid data creation means that storage, trust and protection are paramount, especially for consumer data such as personally identifiable information (PII). In 2017, the average Australian data breach cost organisations AU$139 per compromised record, with financial services and technology businesses experiencing higher than average costs. Nearly half of these data breaches were due to malicious or criminal attacks.[17] One example highlighting the vulnerabilities caused by increased data exchange was the inadvertent release of information on approximately 550,000 prospective blood donors by the Australian Red Cross Blood Service, via a third party provider.[18]

Cyber security opportunities

With data being notoriously easy to copy, modify, falsify or destroy, cyber security solutions are vital to protect any company, customer or collaborator value that may be created by using data. With data often used as an input to decision making for the physical world, cyber security solutions that ensure the integrity of this data is a fundamental need for the safety of people and reliability of systems. Cyber security will empower industry to make increased use of data.

The Australian Notifiable Data Breach scheme, which aims to protect personal information, provides opportunities for cyber security companies to collaborate with businesses to develop innovative solutions to enable safer data exchange.

12 Henke, N., Bughin, J., Chui, M., *et al*. (2016). *The age of analytics: Competing in a data-driven world,* McKinsey Global Institute, [Online] Available from: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world Accessed: 27/02/2017

13 Department of the Prime Minister and Cabinet (n.d.), *Data Integration partnership for Australia,* [Online] Available from: https://www.pmc.gov.au/public-data/data-integration-partnership-australia Accessed: 16/03/2018

14 Zhang X., Liu C., Nepal S., Yang C., Chen J. (2014) *Privacy Preservation over Big Data in Cloud Systems.* In: Nepal S., Pathan M. (eds) Security, Privacy and Trust in Cloud Systems. Springer, Berlin, Heidelberg.

15 CSIRO Futures (2017). *Mining Equipment, Technology and Services – A roadmap for unlocking future growth opportunities for Australia,* Canberra.

16 CSIRO Futures (2017). *Medical Technologies and Pharmaceuticals – A roadmap for unlocking future growth opportunities for Australia,* Canberra.

17 Ponemon Institute (2017). *2017 Cost of Data Breach Study: Australia,* Michigan.

18 Office of the Australian Information Commissioner (2017). *Australian Red Cross Blood Service data breach*, [Online] Available from: https://www.oaic.gov.au/media-and-speeches/statements/australian-red-cross-blood-service-data-breach Accessed: 27/02/2018

2.1.2 ENHANCED EXPERIENCES

Digital technologies are allowing people to have increasingly personalised and enhanced experiences which, in turn, are resulting in changes in human expectations and behaviours.

Customers, communities and employees are demanding more from businesses. These demands will continue to be met through greater integration of digital technologies.

Greater access to information – enabled by improved access to mobile technologies and the internet – is creating more educated and informed decision makers, and changing the experience these users have with organisations. For example, in the healthcare sector, technology and information access are empowering patients to become more proactive in managing their health.[19]

Increasingly, communities and citizens are using social networking platforms to shift public sentiment on issues that are important to them. On average, 6,000 'tweets' are sent every second globally; each having the potential to reach millions of people and dramatically shape perceptions of industry activity.[20] In the oil and gas and mining industries, groups of people can effectively use social media to create strong opposition to business interests, shaping public discourse and influencing businesses social licence to operate.[21]

In sectors such as manufacturing, customers are integrating themselves into the design and decision-making process for goods and services, resulting in output that is customised to their individual requirements – for example, the creation of tailored food ranges.[22]

And technology is also enhancing the way people work by allowing flexible working arrangements, decentralised teams and creating safer work spaces. For example, the use of virtual and augmented reality technologies and robotics can remove the need to have people working in dangerous workplaces.

Cyber security implications

This trend is about enhancing the experience of people; however, it can only be delivered by people permitting increased access to their personal information. Social engineering – the hacking of people – is becoming more sophisticated, with legitimate communications becoming almost indistinguishable from social engineering attempts.[23] Social media and websites provide cybercriminals with personal details to make social engineering attempts appear sincere. Cyber-attacks are increasingly influencing the social world – for example, the interference of a nation state in the 2016 US presidential election by cyber means.[24] With more people using digital technologies and sharing data to enhance their experiences, cyber threats and vulnerabilities are set to increase.

Cyber security opportunities

The intersection of cyber-physical and social systems will drive demand for human-centred security solutions that are useable by all citizens, suitable for social environments, and robust enough to ensure safety and privacy. Cyber security that is managed by humans is not scalable, driving the need for systems and devices that can self-manage their security. Cyber security education and awareness programs for the community are also important and help to promote safe computing practices.

19 CSIRO Futures (2017). *Medical Technologies and Pharmaceuticals – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
20 Glindemann, R. (2017). *Galvanising the opposition: social media campaigns and the new risks for the oil and gas industry*, The APPEA Journal 2017, 57, 448–451.
21 CSIRO Futures (2017). *Oil and Gas – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
22 CSIRO Futures (2017). *Food and Agribusiness – A roadmap for unlocking value-adding growth opportunities for Australia,* Canberra.
23 Australian Cyber Security Centre (2017). *ACSC Threat Report 2017, p. 29.*
24 Australian Strategic Policy Institute (2017). *Cyber maturity in the Asia–Pacific Region 2017,* Barton.

2.1.3 GLOBALLY CONNECTED

Global connection through the digital world is enabling trade; empowering people with access to information and novel products and services; and allowing seamless communication for improved social connections.

A digital world is inherently borderless and increases the opportunity for industry growth in both mature and emerging economies by allowing end users and businesses to connect with their ecosystems from any location. It also opens up new markets, which allows for new product development and innovation. Digital connectivity also provides options for new market entrants to gain a foothold to quickly access global markets, thereby competing with longstanding incumbents.

The Internet of Things (IoT) is an umbrella term that describes the billions of physical devices around the world that now connect to the internet and to each other. When implemented constructively, IoT has a positive impact on the three other trends identified. It is a term used to describe everything from a lightbulb controlled by a smartphone app to a driverless freight train.

Digital technologies are also changing the way the global workforce interacts with employers. Remotely-controlled facilities, automation, virtual and augmented reality, and cloud computing are all technologies that are changing the future of work. These technologies are enabling faster, safer and more efficient completion of tasks, sometimes with the help of robotics and a non-local workforce.

Cyber security implications

Greater global connection means that cyber-attacks can come from anywhere in the world. The WannaCry ransomware attack in 2017 demonstrates the global nature of cyber security threats affecting organisations in over 150 countries. Across the world, the nature of workplaces are being transformed by IoT technology, with remote connection of physical devices introducing new cyber security and cyber-physical risks that need to be addressed. Authentication and security of these physical devices need to be addressed in order to lessen the impact cyber-attacks can have in the physical world.

Cyber security opportunities

For global connectivity to add value to businesses and people, cyber security solutions must maintain authenticity, privacy and integrity of global engagements and communications. Solutions will need to focus on providing a clear indication of data provenance, confidence in cross-jurisdictional collaboration and rapid sharing of relevant cyber security threats. Greater connectivity globally also means that threat-sharing collaboration needs to improve, thus allowing quick assessment and mitigation activities to be undertaken. With cloud-based technologies being a key enabler of global workforces, development of cloud-based security and privacy solutions for devices is needed.

2.1.4 TRANSFORMED SUPPLY CHAINS

Digital technologies are transforming supply chains, creating greater transparency, increasing efficiencies and blurring traditional boundaries.

Supply chains across industries are evolving and transforming in three key ways:

- Firstly, there is a greater focus on the end user, with supply chains adapting to develop products and services that are more closely aligned to meet customer's needs. This is changing the traditional role some businesses play in supply chains. For example, some manufacturers are expanding their role from making 'widgets' to developing tightly-integrated, product-service bundles.[25]
- Secondly, the adoption of digital technologies is leading to a seamless exchange of information between businesses, suppliers and consumers, which is creating new opportunities for collaboration, specialisation, and vertical integration. Automation is also creating new opportunities for increased efficiencies and optimisation of supply chains.
- Thirdly, access to global supply chains will continue to create new market opportunities while at the same time, introducing new competition and supply risks.[26]

In addition to traditional supply chains, a completely new form of supply chain has emerged and underpins all others – the information supply chain.

An evolving cyber security threat landscape

With constant innovation, barriers to entry for engaging in malicious cyber activity are low. Cybercrime has become a low-risk, high-reward business model with an estimated 20:1 profit to effort ratio, resulting in a proliferation of low-end actors.[29] Changes in technology also mean that high-end actors, such as nation-states and criminal groups are more powerful and sophisticated than ever before. The growing strength and proliferation of cybercrime, converging with the impact of new digital trends, mean there has never been a more important time for Australian organisations to invest in cyber security to enable their ongoing innovation and growth, and to keep employees and the community safe.

Cyber security implications

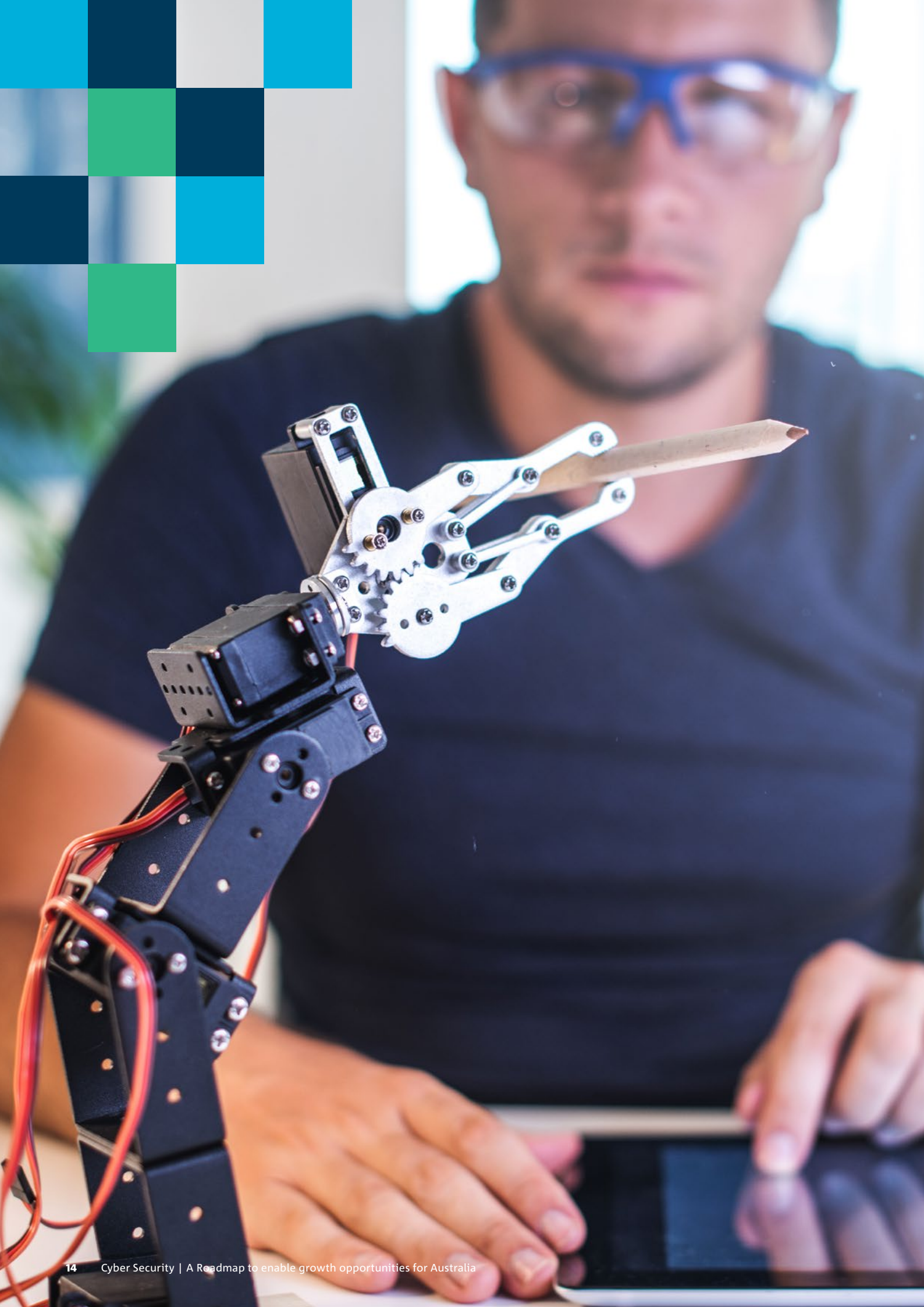
Supply chains are critical to business operations and are a high-value target for cybercriminals. As cyber security defences improve, adversaries will seek secondary or tertiary access to primary targets through contractors, supply chains or other third parties.[27] These parties often have trusted relationships with the primary target and hence are provided with extensive access.

Cyber security implications to supply chains are three-fold: (1) disruptions to downstream businesses caused by upstream interruptions, (2) the rapid dissemination of cyber threats via the information supply chain, and (3) the potential loss of Intellectual Property (IP) with unsecure supply chain partners.

Cyber security opportunities

The physical supply chain already presents complex challenges for businesses; digitisation and automation of the process adds an extra layer of complexity. Cyber security solutions are essential for protecting the transfer, availability and integrity of data across supply chains. As the dependence on digital technologies and integration of supply chains increases, the possibility for cyber-attacks grows, spurring demand for innovative security solutions that create a trusted supply chain and protect IP. Supply chains are a promising domain for the application of blockchain technology.[28] Building trust in global supply chains and trade will be an important role for Australia's cyber security sector.

25 CSIRO Futures (2016). *Advanced Manufacturing – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
26 CSIRO Futures (2017). *Food and Agribusiness – A roadmap for unlocking value-adding growth opportunities for Australia,* Canberra.
27 Australian Cyber Security Centre (2017). ACSC Threat Report 2017.
28 Staples, M., et al (2017). *Risks and opportunities for systems using blockchain and smart contracts,* Data61 (CSIRO), Sydney.
29 Cisco Umbrella (2016). *Economics of cybercrime – The evolving cybercriminal business model.*



Cyber security growth themes

3 Cyber security growth themes

Cyber security needs to be viewed as a growth-enabling activity if Australian businesses want to remain competitive in an increasingly digital environment.

Following on from diverse industry consultation, three themes have emerged in relation to understanding how cyber security solutions can lead to more effective organisation and business operations, and thus improve Australia's overall cyber security posture to take advantage of digital transformation. The themes cut across sectors, and build on the dialogue presented in Australia's Cyber Security Strategy and Australia's International Cyber Engagement Strategy by discussing how Australia can embed cyber secure behaviour through building trust, improving design processes and raising overall cyber resilience.

Technology alone will not provide the solution and the growth themes present behavioural changes, as well as discussing organisation guidelines and training activities that will lead to a cyber secure culture. These broadly align with and confirm the technology, process and people triad that is often discussed as being key to the success of information technology. Importantly, these themes build on the goals established by AustCyber to (1) grow an Australian cyber security ecosystem, (2) export Australia's cyber security to the world and (3) make Australia the leading centre for cyber education.

FIGURE 4: GROWTH THEMES FOR CYBER SECURITY

3.1 Theme 1: Trusted ecosystem

Creating digital ecosystems that are highly trustworthy, allowing for rapid exchange of information and providing a stronger environment for trade.

Australian industry must consider the requirement for secure data and information sharing to ensure that local, domestic and international trade is not restricted by concerns over the integrity of data or the trustworthiness and reliability of trading partners.

Creating a trusted ecosystem for the rapid and reliable exchange of information will involve the development of cyber security strategies and solutions that will allow for increased collaboration between stakeholders across Australia's priority sectors. The development of a trusted ecosystem will be particularly challenging for sectors that are heavily fragmented (i.e. those with a large number of start-ups and SMEs).

Access to international supply chains is critical for the success of Australian businesses as the local market is often too small to allow them to reach sustainable scale. International cyber-engagement and maturity of Australian trade partners has been given considerable attention by the Department of Foreign Affairs and Trade (DFAT's Australia's International Cyber Engagement Strategy) and the Australian Strategic Policy Institute (ASPI Cyber Maturity in the Asia-Pacific Region 2017). These bodies of work establish important parameters for the development of a trusted ecosystem. Importantly, any frameworks that are developed locally for international trade should not detract from existing agreements.

To effectively develop a trusted ecosystem, the cyber security sector and the priority growth sectors will be required to collaborate in order to develop an understanding of how to achieve the following visions:

- **Trusted partners**
  Market forces will lead to systems that facilitate user-friendly and trusted sharing of information within supply chains, with third parties and with customers. These systems will ensure only authorised and trusted users have access to information, and will help to ensure that third parties do not introduce new risks into organisations. The need for innovative ways to authenticate trusted partners will create opportunities for the cyber security industry. Short-term developments must focus on the needs of specific industries, with cross-industry structures emerging over time.
- **Threat intelligence sharing**
  Information about cyber threats is shared within industry efficiently, thereby allowing credible threats to be identified and risks to be quickly understood. Appropriate systems are in place to protect the confidentiality of reporting organisations (where necessary) and the integrity of the information, with incentives to encourage the appropriate level of threat intelligence sharing within and across sectors creating a 'competitors as collaborators' mindset.
- **Collaborative demonstration projects**
  Demonstration projects aim to illustrate how a trusted system may be established to create commercial value within Australia's priority growth sectors. These projects involve a small number of businesses of various sizes and their supply chains in collaboration with innovative cyber security organisations. Australia's small but well-developed market provides an exemplary testing ground for pilot programs to then be rolled out in larger economies.
- **Resources and guidelines**
  Best-practice guidelines and tailored cyber security assessment resources are available that are customised to Australia's various industries and adaptable to the unique circumstances of businesses (large and small). Resources include information and templates which help organisations build safe practices to engage with other businesses in a trusted way, and guidelines that incorporate frameworks for incentives to motivate adoption.

- **Onshore capability**
  While imported off-the-shelf solutions can be more accessible, Australian organisations are encouraged in the direction of co-investment and judicious procurement of locally-developed cyber security solutions where suitable and available. Together with a concentrated effort to grow the Australian cyber security sector, this will help the nation to develop and maintain a critical mass of onshore cyber security capabilities which, in turn, is paramount to building a trusted local ecosystem and reinforcing the trust associated with 'Brand Australia' in a digitally-connected global economy.

Australia's small but well-developed market provides an exemplary testing ground for pilot programs to then be rolled out in larger economies.

The motivation for competitors to collaborate against cyber threats

A trusted ecosystem can be developed by sharing threat information and working collaboratively with industry peers and government to understand the most appropriate methods to mitigate threats. In the Australian financial services and banking sectors, information regarding cyber security is shared between competing organisations through communities such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). This occurs as each organisation understands that the net benefit of collaborating to mitigate existing and emerging cyber threats is significantly greater than attempting to do so alone.

The rationale behind this is straightforward: while a successfully deployed attack on a single major financial or banking institute would destroy its brand and reputation overnight, there is a very high chance that the same attack method may be successful for multiple institutions, which means they are all vulnerable to losing significant value. Research suggests that 61% of customers would stop using a business's products or services if a cyber-attack resulted in a known security breach.[30] Even in the event that the competing institutions are not vulnerable to the same attack, the public perception of the entire sector will have been tarnished. This means that the entire financial and banking sector has significant value-based motivation to ensure that they openly share and understand cyber threats.

Translating this behaviour to other sectors in Australia is not straightforward. There are many challenges that need to be overcome: competitive industries often do not share information where commercial gain is not clear; there may be legal and privacy restrictions on what can be shared; and there is a potential for reputational risk. Building a culture involving sharing threat information whereby one organisation's detection of a threat can lead others to successful mitigation will require significant industry maturity.

Industries such as food and agribusiness generally lack the digital maturity required to effectively assess their threat landscape, and generally do not share cyber threat information. Federal legislation such as the Notifiable Data Breach Scheme will provide motivation to increase threat information sharing within a sector; however, it is based on driving compliance rather than protecting and increasing value within a sector. Overcoming this provides an opportunity for purposeful inter- and intra-sector collaboration.

30 PWC (2016), Digital trust Securing your future in the digital world, [Online] Available from: https://takecontrol.pwc.com.au/digital-trust/ Accessed: 05/03/2018

3.2 Theme 2: Secure by design

Ensuring new products, services, platforms and processes are designed with cyber security as a key consideration.

IoT devices are often insecure by design which creates significant vulnerabilities in the community.[31] It is essential that cyber security implications are considered early in the design phase of all new technologies, processes and systems. Rigorous early assessment of cyber security vulnerabilities allows for adaptable security measures and helps to define how much effort should be expended on overcoming a particular vulnerability. This is critical as security has a cost associated with it, and hence the value gained from incorporating security needs to be balanced and understood early in the development process.

Incorporating secure by design principles and implementing good cyber security practices will, over time, allow Australian organisations to create a competitive advantage for products and platforms that are developed onshore. As cyber security solutions move from being a post-development consideration to a design-phase consideration that is tightly integrated with the industry vertical, time to market will improve, as will the reputation of the products and services being developed in Australia. Secure by design will also underpin the long-term objectives of building a trusted ecosystem and a robust and resilient industry, thereby allowing Australian organisations to build a business model and competitive advantage around strong cyber security practices.

As cyber security solutions move from being a post-development consideration to a design-phase consideration that is tightly integrated with the industry vertical, time to market will improve, as will reputation of the products and services being developed in Australia.

Industry examples of secure by design

IoT device development considers hardware and software strengths and weaknesses, and the vulnerabilities that may occur once the device is embedded into a local system.

Public infrastructure implementation considers how cyber security measures can be used to improve the effectiveness, resilience and adaptability of the infrastructure.

Supply chain design considers the trustworthiness and reliability of partners from a cyber security point of view, and includes process development to improve robustness.

Governments and multinational organisations consider the implications of partner jurisdictions legislation concerning cyber security during trade negotiations.

This growth theme is particularly important for Australian organisations that are involved in the development of critical technology and infrastructure. For example, development of energy supply infrastructure and health services must consider cyber security vulnerabilities, where previously this would have received minimal attention. Enabling this theme requires a broader understanding of cyber security by the priority growth sectors. Visions for this theme include:

- **Assurance of secure products**
  Guidelines establish a baseline for built-in cyber security in products and services that harmonises with international standards, thus allowing for improved exportability. A strategy to communicate this feature to consumers is in place, with messaging that ensures secure by design principals add value to both the user/consumer and the developer. Such a strategy should transcend the notion of a quality assurance 'tick' to further encourage innovation and deepen a risk-focused security culture in users/consumers (rather than incentivise complacent behaviours).

31 Korzeniowski, P. (2018). *Internet of Things (IoT) technologies for process manufacturing: global markets*, BCC Research.

- **Secure by design skills in workplaces**
  The cyber security industry helps organisations improve their workplace skills, ensuring strategies are tailored to various roles within companies by highlighting the role each person plays in keeping a company secure and resilient. Companies involved in the development and commercialisation of new technologies and early-stage product and platform development have strong cyber security practices and skills, and are able to embed cyber security early in the design process for new products and services.
- **Security embedded in ICT training**
  The gap between cyber security and ICT education is bridged by embedding more cyber security aspects into all tertiary information technology courses, with the foundations of the cyber security content centred around the interdisciplinary nature of the economy's skills needs.
- **Research and industry collaboration**
  As Australia's priority sectors address their challenges and capitalise on growth opportunities, Australia's cyber security sector and the research community collaborate to help Australian industry underpin innovation with strong cyber security.
- **Secure trade and supply chains**
  Contractual negotiations and trade agreements clearly integrate cyber security measures in the development phase, leading to much greater security across supply chains. This can be applied at the local, national, international or inter-government level.

Guidance on securing the design of medical wireless infusion pumps and mobile data sharing

The National Cybersecurity Center of Excellence (NCCoE) in the United States – a part of the National Institute of Standards and Technology (NIST) – has developed a number of use cases to tackle industry-specific cyber security challenges. Across many use cases, the NCCoE has developed special publications to help improve cyber security in these industries, which can be adapted to similar industries outside the USA, including Australia. One key focus area has been in the healthcare industry: in particular, helping organisations secure wireless infusion pumps and electronic health records on mobile devices.

The NCCoE recognised that medical devices are no longer stand-alone instruments; instead, they are connected to a variety of other systems, networks and devices. While this connection can improve healthcare delivery, it also exposes organisations to serious risk factors such as access by malicious actors, breach of protected health information and loss or disruption of healthcare services.

Similarly, the NCCoE observed that the use of mobile devices to store, access, and transmit electronic healthcare records is outpacing the privacy and security protections on those devices which, in turn, poses risks around privacy of data and medical identify theft.

These two use cases have resulted in the development of the following special publications:

- NIST Cybersecurity Practice Guide SP 1800-1, Electronic Health Records on Mobile Devices
- NIST Cybersecurity Practice Guide SP 1800-8, Wireless Infusion Pumps.

These publications provide best practice and detailed 'how to' guidance to help companies improve cyber security principles in the design of their products and platforms.[32]

32 National Cybersecurity Center of Excellence (n.d.). *Healthcare Sector Use Cases,* National Institute of Standards and Technology (NIST), [Online] Available from: https://www.nccoe.nist.gov/projects/use-cases/health-it Accessed: 6/03/2018

3.3 Theme 3: Robust and resilient

Building greater cyber maturity and resilience in Australian industry and communities by developing a robust security culture.

International cyber security practices are yet to reach a uniform level, providing Australia with an opportunity to position itself as a best-practice nation for cyber security. However, moving Australian industry from its current state to one where all businesses demonstrate a sophisticated, robust and resilient security culture will require cultural change.

Australia's priority sectors can lead the way by working with cyber security businesses and researchers to develop unique solutions that improve the way they approach cyber security. Furthermore, improving the baseline national awareness and approaches to cyber security could see a significant increase in consumer confidence and business performance. In addition to improving the prevention of cyber-attacks, robust solutions for rapid recovery and forensics will see companies not only preventing more attacks, but when attacks do occur, being in a position to recover from them faster.

Importantly, the unique attributes of each sector will help define the specific activities that allow for improved overarching approaches to cyber security. While there is a baseline commonality to the cyber threat landscape, a nuanced approach is needed. At the more sophisticated level, different industries face different types of threats. While improving the ability to detect and defend against complex malicious attacks is critical for financial institutes, at this stage it is the more prosaic attacks via unpatched systems or network vulnerabilities that leave other sectors at risk and decrease their growth potential.

To effectively develop cyber maturity in Australian industry, the cyber security sector and the priority growth sectors will be required to develop sustained methods for achieving the following visions:

- **Awareness in the community**
  Community awareness concerning the importance of cyber security practices is strong and is supported by a targeted, high-profile education campaign (similar to the famed national 'Slip Slop Slap' skin cancer campaign). The call to action drives the community to learn security basics and procure trusted solutions to protect themselves. Safe behaviours online are developed as individuals have a better understanding of the cyber security risk they face in their homes and workplaces.
- **Workforce skills**
  Awareness of cyber security basics in the context of workplaces is strong throughout all levels of staff, with companies adopting appropriate risk-based practices such as the Australian Government's Essential Eight set of security practices. At the Executive and Board of Directors level, there is an enhanced level of understanding about the importance of enterprise-wide security culture, with incentives that reward good practice and support investment in leading technologies. Cyber security education and skills delivery in all education institutions (tertiary, secondary and primary) is improved through the development of slot-in modules and materials for programs across all disciplines. Where possible, these modules should incorporate elements of workplace learning.

- **Frameworks for cyber security**
  New frameworks and improved governance enables Australian industries to be more innovative and experiment with new products, services and emerging disruptive technologies in a timely and safe fashion. The frameworks will allow the cyber security sector to truly enable industry innovation, while ensuring cyber resilience is prioritised. These frameworks are customised to the applicable industry and are regularly updated to evolve with levels of maturity, changing technologies and emerging trends.
- **Strong leadership**
  Executive and Board level cyber security literacy and education initiatives through peak bodies and other organisations are supported and well attended. Leadership teams consider cyber security as a strategic priority and an innovation enabler, rather than a cost, across all areas of business.
- **Australia's reputation**
  Australia's cyber security sector – in collaboration with the priority sectors – has built a national reputation for cyber security excellence, leveraging the strengths of the research community and industry. Importantly, Australia's reputation is focused on excellence across key cyber security pillars. For example, these might include quantum technology, wireless technology, trustworthy systems and niche high-value hardware.[33]
- **Universal cyber care**
  Technology solutions focused on helping to raise the general cyber security hygiene of the Australian public and businesses have been investigated and developed. Potential options for this may include, for example, subsidised access for SMEs and households to a router-like device that provides a resilient and patchable network environment which safeguards against the majority of vulnerabilities; the provision of subsidised cyber security expertise; or free secure cloud storage for users to back up devices and data regularly.

Topic for debate – Clean internet

The central point of the robust and resilient theme is to raise the quality of the approach that Australia takes against cyber threats by promoting and enabling industry actions that make all environments intrinsically secure. The bulk of cyber threats to businesses and households have been created by increased connectivity, with malicious actors using simple and readily available technologies to take advantage of devices that have poor cyber security. Building on the concept of 'universal cyber care' is the idea of providing all Australians with clean internet which, in theory, could mitigate the majority of cyber threats posed to Australians. This could be implemented in a number of ways, such as a national opt-out scheme that automatically enrols every internet connection to a clean gateway.

The counter argument to this is that it may restrict freedom on the internet, and that each individual or business should choose and implement their own solution to enable a cyber secure environment. This market-driven approach works well in the cultural context of a country such as Australia, but does require considerable effort to be made to ensure that the right environment is cultivated to allow the market to deliver accessible and useful cyber security solutions.

AustCyber is well positioned in its role as an independent sector advocate to lead the debate on whole of economy issues, such as clean internet, and the potential impact that both possibilities could have on Australia.

33 Australian Government (2015). *Science and Research Priorities Cyber Security – Capability Statement* [Online] Available from: http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Documents/Science-Research-Priorities-Cybersecurity.pdf Accessed: 27/02/2018

Addressing the cyber security skills gap

Addressing the expected skills gap in cyber security is critical to the successful growth of robust and resilient Australian industries. It is expected that Australia will need between 11,000 to 18,000 additional cyber security workers over the next decade. To help address this shortage, TAFEs across Australia have joined forces to begin delivering Australia's first national skills-based cyber security Certificate and Diploma level qualifications. The Certificate IV in Cyber Security and Advanced Diploma of Cyber Security courses are practical, non-degree courses that students can complete on-the-job. These courses will open pathways to learners seeking further education and a potential new career meeting the security challenges faced by Australian employers.[34]

Further ways to address the cyber security skills gap are addressed in AustCyber's Cyber Security Sector Competitiveness Plan.

3.4 Enabling actions for cyber security growth

Realising the themes to achieve the overarching vision requires change via collaborative action with the Australian cyber community working closely with businesses, research institutes, governments, industry associations and the Industry Growth Centres. Presented over the immediate, short (1 – 3 years) and medium terms (3 – 5 years), each set of actions is aligned to one or more of the themes (as indicated by each icon).

Many of the immediate actions are already underway in cyber literate sectors such as finance and defence, but require further consideration in order to be implemented across broader Australian industry. Collectively, these actions support and enhance a coordinated national approach to industry's contribution to raising Australia's cyber security resilience.

34 AustCyber (2018). *Media Release: Australian TAFEs Join Forces to Tackle the Cyber Security Skills Gap,* [Online] Available from: https://www.acsgn.com/wp-content/uploads/2018/01/ACSGN-TAFE-Media-Release.pdf Accessed: 07/03/2018

Enabling actions for cyber security growth

IMMEDIATE

Guidelines and frameworks

Improve guidelines for best-practice cyber security hygiene

Work with Australian priority industries to develop guidelines for best-practice cyber security hygiene that are harmonised with key international guidance and standards to ensure commercial interoperability and global market access (e.g. NIST and ISO in the US and EU respectively). These guidelines should take into account the Australian Government's Essential Eight set of security practices, and the Office of the Australian Information Commissioner's data privacy guidelines to help businesses define and classify data, identify vulnerabilities in processes, and recommend minimum practices that will help to protect data and manage the supply chain implications of cyber threats. Guidelines should also help companies understand the importance of both sharing threat intelligence and monitoring information-sharing networks. These guidelines will need to be adapted to each industry while providing for a baseline of common practice.

Threat intelligence sharing

Improve shared threat intelligence within Australian industries

Facilitate the development of sector-specific networks that allow for the rapid dissemination of highly applicable and tailored information about existing and potential cyber security threats, and recommended mitigation strategies. This action will need to leverage existing platforms such as CERT Australia, the Australian Cybercrime Online Reporting Network (ACORN), JCSC, the Trusted Information Sharing Network (TISN), and the various Information Sharing and Analysis Centres, together with industry organisations such as the Industry Growth Centres. This action should also seek to streamline and evolve existing platforms as a means to incorporate agile and efficient technologies. Development of these networks will require education concerning the importance of disclosing information about cyber security breaches for greater economic benefits.

Skills and training

Improve basic cyber security practices

Help organisations adopt basic cyber security hygiene and ensure safe computing practices are embedded throughout all levels of the organisation.

Improve cyber literacy in company leadership structures

Boardroom leadership in the implementation of cyber security strategies within organisations is essential. The cyber security sector must develop resources and education opportunities to help improve the cyber security literacy of company executives and board directors. Leadership must have a better understanding of cyber security implications and risks within their business. Education initiatives, tailored by industry, will help to improve cyber leadership across Australian industries and improve adoption of cyber security solutions.

(For more on skills and training initiatives – see AustCyber's SCP 2018 update)

Trusted ecosystem | Secure by design | Robust and resilient

SHORT TERM (1-3 YEARS)

Develop data sharing frameworks

Work with industry sectors to develop and implement frameworks to help specify ownership, privacy and security considerations. This will enable collaborative data sharing within industry and along supply chains for bespoke opportunities. The frameworks will take into account global norms of behaviour online, international law and market entry requirements, including export control treaties. The Office of the Australian Information Commissioner (OAIC) has developed a series of privacy guidelines that can be built on for ownership and security frameworks.

Improve baseline device and platform security

Develop frameworks with recommendations for baseline cyber security that should be built into any platforms or devices that capture and transmit data. This could be part of an international effort to better manage ICT supply chains using Australia as a test case.

Build 'secure by design' workforce skills

Upskill staff working on digital technology development and deployment across priority sectors with the skills needed to assess the need for cyber security early in the design process. Bring in cyber security developers/ consultants early in the product development lifecycle.

Embed cyber skills into ICT workforce

Traditional ICT courses and training have limited focus on security. Fundamentals of cyber security to be embedded into traditional tertiary and vocational information technology courses.

MEDIUM TERM (3 – 5 YEARS)

Develop agile frameworks for technology adoption

Develop suitable frameworks and governance to enable the safe and effective adoption of emerging technologies into industry, thereby ensuring cyber resilience is prioritised. These frameworks need to be customised to Australian industry and need to be regularly updated to evolve with changing technologies and trends.

Improve frameworks for international trade

Construct a framework to assist in negotiations for international trade. Frameworks should establish a shared understanding of minimum acceptable cyber security practices, risks and responsibilities concerning data and information exchange. They should also incentivise markets to favour innovative solutions.

Improve global threat intelligence sharing

Increase engagement with international companies and governments with a goal of sharing information about cyber security threats and vulnerabilities. Look to leverage the expertise of the research community in this effort to ensure an 'over the horizon' perspective is built in.

Embed cyber skills into general workforce development

Develop drop-in modules focused on cyber security for traditional university feeder degrees for industry.

Create active education experiences

Work with businesses to create immersive education scenarios to be played out on-site, with the aim of developing greater organisational awareness and understanding of the impact everyday activities can have on the cyber security risk profile of the business.

IMMEDIATE

Cyber security awareness

Develop business awareness and cyber resources

In collaboration with interested industry associations and industry growth centres, develop regular cyber security awareness events and webinars tailored to organisations in different industries.
Develop resources to help organisations (in particular SMEs) plan their cyber security strategy to complement digital transformation strategies. These resources should be adaptable to individual organisations and provide information on how to embed good security practices into all business processes, from hiring and training new staff to supply chain cyber security assessments. SME awareness events might leverage the Entrepreneurs' Programme cyber security webinars and resources could leverage the tools and resources provided by the Australian Government's business.gov.au online resource.

Build community awareness

Develop a national awareness campaign for safe computing practices aimed at the general community, primary and secondary education students. This campaign should feature cyber security as an essential step in the safe use of digital technologies in the home. It should provide easy-to-implement actions and direct the community to learn security basics and procure solutions for increased protection. This campaign might build on the Safer Internet Day (SID) and the Stay Smart Online Week events that are held annually.

Celebrate home grown cyber solutions

Develop materials for case studies and celebrate the success of Australian developed cyber security solutions to help boost Australian procurement of locally made solutions.

Collaboration with Australia's growth industries

Establish demonstration projects

Establish collaborative demonstration projects that encourage a consortium of participants from across a sector to trial and demonstrate ways that data and practices can be beneficially shared among participants in a secure and trusted fashion.

Improved cyber-physical systems

Develop solutions for areas of poor connectivity

Access to telecommunication infrastructure is improving across Australia, with mobile internet and high speed broadband networks expanding. However, full connectively remains out of reach to a number of entities. Cyber security needs to be considered when new solutions are being developed to help companies operating with disjointed or poor connectivity in both rural and urban areas.

SHORT TERM (1-3 YEARS)

MEDIUM TERM (3 – 5 YEARS)

Improve communication of secure by design features

As secure by design practices become commonplace, communication of this baseline security can help build Australia's competitive advantage. Create a communication and messaging campaign that helps buyers and consumers easily recognise products that have strong built-in security features. Further industry consultation around the framework for this messaging is required.

Build solutions for Australia's growth industries

As Australia's priority growth industries capitalise on opportunities for digital growth, the cyber security sector must simultaneously work with forward thinking companies to develop domain expertise and bespoke solutions that enable and capture value from industry momentum and growth. Working collaboratively with these growth industries and developing relevant expertise and solutions will help the cyber security sector grow and develop exportable solutions.

Build Australian exports and global reputation

Help to build Australia's reputation for cyber security by investing in innovative security projects to enable consistent deployment of intrinsic security into Australian manufactured and developed digital products and services. As Australian industry develops a reputation for excellence in secure by design principles, export demand will be stimulated across priority sectors.

Ensure cyber security is considered in trade negotiations

Work with organisations to ensure that cyber security implications are addressed up-front in contractual negotiations for trade, ensuring a secure global supply chain.

Transform business models

Assist businesses to integrate secure by design principals into product and service development, alongside other cyber security solutions. This will help businesses develop stronger value propositions, with cyber security helping to transform and improve business models.

Mitigate legacy systems risk

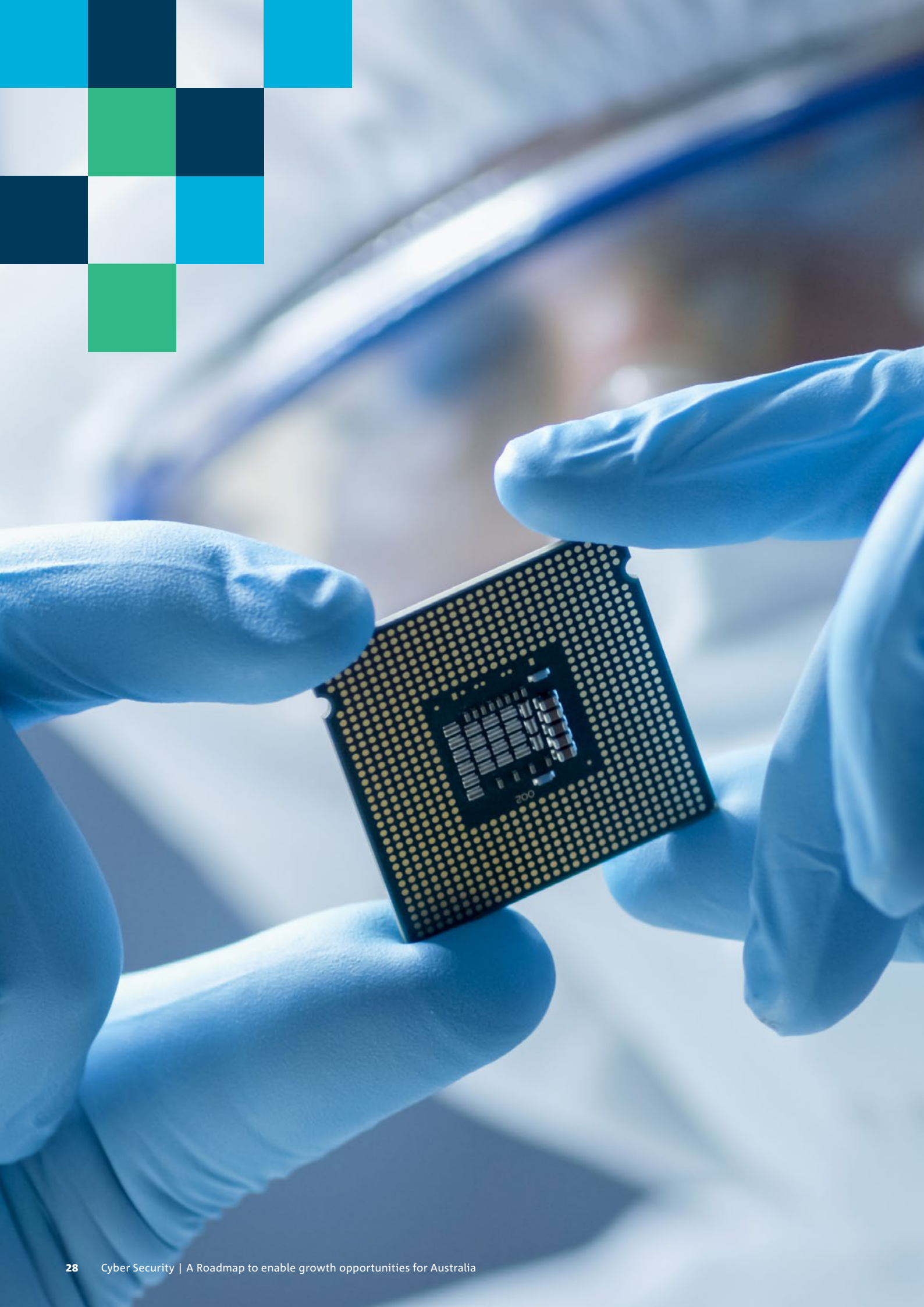
Operational technology environments have historically been isolated from other networks and have few safeguards. Solutions are required to improve the safe integration of operational technology with business systems.

Improve data collection

The quality and integrity of data collected from various connected equipment and sensors is variable. To help address the challenge of trusting this information for decision-making, data-handling protocols, and quality standards for improvements to sensors and data collection technologies are required.

Establish trusted inter-site networks

Implement fit for purpose secure networks for sub-segments of an industry with shared interests and goals, providing enhanced utility of data and avenues for new modes of collaboration.



Cyber security for Australia's priority sectors

4 Cyber security for Australia's priority sectors

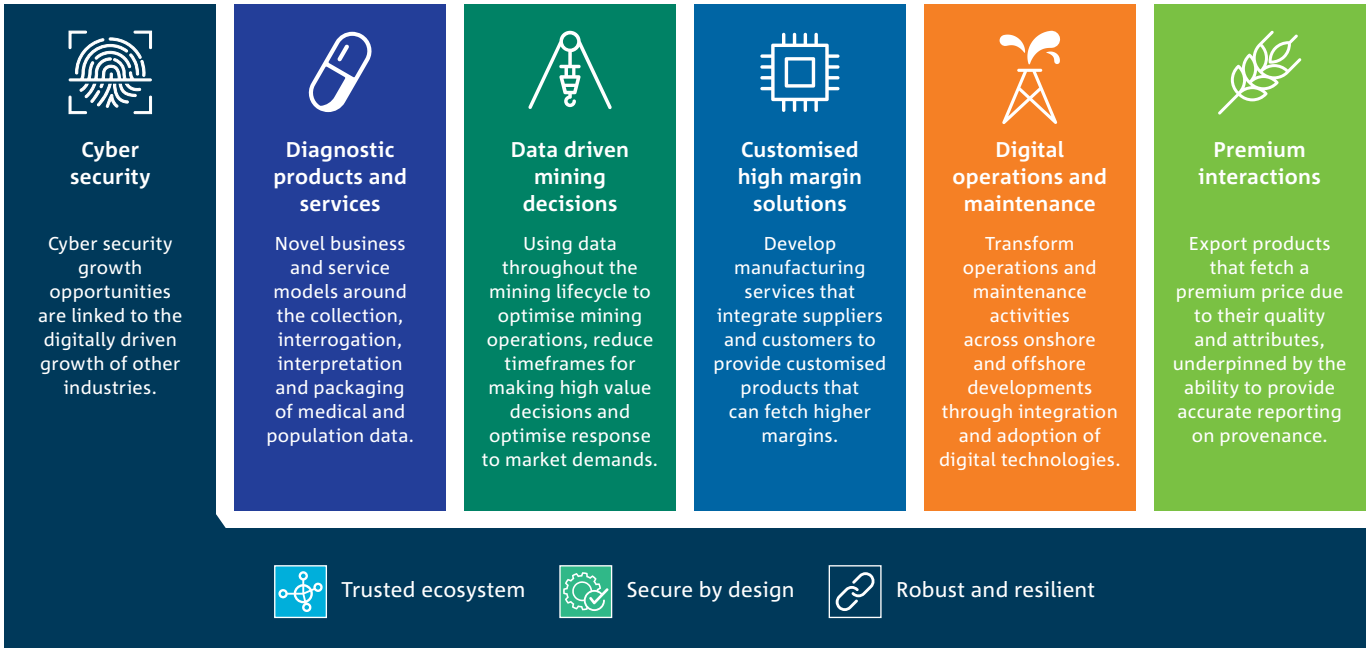
> "For Australia to be globally competitive, cyber security must underpin the data-driven transition of every sector in the economy." Australia's Cyber Security Strategy[35]

To be truly effective, Australian industry and the cyber community must tailor the enabling themes and actions presented in this Roadmap to each industry's specific opportunities for growth. By unpacking growth opportunities presented within the themes in this report, Australian industry and the cyber security sector can both work towards the development of competitive offerings for local and international markets.

This chapter focuses on addressing the cyber security requirements needed to enable a selected growth opportunity from each of CSIRO's Industry Roadmaps (Figure 5). In doing so, a framework has been developed (Figure 6) which can be readily applied to other opportunities within these sectors, as well as for sectors that have not been considered here.

While the actions identified in Chapter 3 will go a long way towards improving the cyber resilience of Australian industries, this chapter identifies priority actions and future research priorities for each sector. These actions span the various themes, and require collaboration between the cyber security sector and the industry in question, alongside research and government support. Collaborative projects that seek to address the research priorities could leverage existing funding arrangements, such as AustCyber's Project Fund.

FIGURE 5: AUSTRALIA'S STRATEGIC PRIORITY SECTORS AND SELECTED GROWTH OPPORTUNITIES



35 Department of the Prime Minister and Cabinet (2017). *Australia's Cyber Security Strategy – First Annual Update*, Commonwealth of Australia, [Online] Available from: https://cybersecuritystrategy.pmc.gov.au/first-annual-update/cyber-landscape.html Accessed 27/02/2018

FIGURE 6: FRAMEWORK FOR OPPORTUNITY INVESTIGATION

Industry opportunity

- What is the industry opportunity, and how does the opportunity leverage connectivity, cyber-physical systems, data, etc.?
- What motivations are there for a cyber attack in this industry, or specifically, for this growth opportunity?

Value development

Cyber security challenges

- How does this opportunity create value for the customer, the company and collaborators?
- What are the cyber security implications and challenges associated with protecting this value?

Cyber secure vision

- Using the themes of ecosystem trust, secure by design, and robust and resilient as a guide, what does a cyber secure future look like for this opportunity?

Priority actions

- What are the priority actions that need to be addressed to achieve the vision; what existing initiatives can these build from?
- What research and development needs to be undertaken?

By understanding the growth opportunities that industries are likely to pursue and focusing on Australia's strengths, the Australian cyber security sector is able to proactively develop tailored solutions and develop competitive exportable offerings for a global marketplace.

Australia's medical technologies and pharmaceuticals industry (MTP)

4.1 Australia's medical technologies and pharmaceuticals industry (MTP)

4.1.1 DIAGNOSTIC PRODUCTS AND SERVICES

Precision health and the provision of patient-centric health and medical solutions will be based on the ability of research organisations and companies to effectively leverage the increasing volumes of health, population and medical data being generated. Australia's MTP industry has an opportunity to lead the way in the development of diagnostic platforms and precision medical solutions.[36]

Over the past decade, there has been an explosion in the variety and volume of health data generated and collected by Australia's healthcare system, and by patients themselves. This data originates from multiple sources, including diagnostic platforms such as medical imaging and genome sequencing, electronic health records, and non-clinical data collected from wearable devices and mobile device apps. To date, this data has not been effectively leveraged. Rather, it has been waiting on better integration with a broader set of patient, population and environmental information – a challenge that has nuanced quality, security and integration requirements.

Using a clear framework for privacy-preserving techniques on patient data, the Australian MTP industry has the opportunity to develop novel business and service models associated with the collection, interrogation, interpretation, and packaging of medical and population data. This will promote innovation and improvement of regulated and consumer diagnostic products and services, and enable the development of precision and preventative health solutions.

Patients sometimes withhold critical information from healthcare providers due to concern that their records could be breached.[37]

Electronic heath records will provide a platform for innovation in digital apps and tools to support health and wellbeing.[38]

It is important that the MTP sector maintains a social licence and community trust for the collection, ownership and use of patient data, both de-identified and identified. In a low trust environment, patients and data custodians will have heightened concerns over loss of control of data, loss of economic or personal value, and fears of adverse or unintended outcomes.[39] Failure by the MTP sector to ensure appropriate cyber security is built into medical devices, alongside development of safeguards, transparency and effective risk management for medical data, will result in loss of community trust and acceptance.[40]

Motivations for cybercrime in healthcare are wide-ranging, from causing disruptions for thrill-seeking reasons, to monetary gain via blackmail or leveraging the value of patient health data on the black market. Because of these motivations and their impact on privacy and safety, cyber security solutions are critical and will underpin the confidence required to allow increased access to patient and population data, and innovation in connected medical devices that capture and use data. The benefits and value gained from data sharing need to continue to outweigh the risks to privacy, confidentiality and security.

The opportunity to lead the way in the development of diagnostic platforms and precision medical solutions is driven by a global need to improve the effectiveness of health care, and is made possible by advances in data generation, privacy, security and interoperability. It builds value by providing avenues for improved patient outcomes, increased cost effectiveness for healthcare delivery, and novel commercial solutions.

36 CSIRO Futures (2017). *Medical Technologies and Pharmaceuticals – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
37 Australian Digital Health Agency (2017). *Information Security Guide for small healthcare businesses,* Commonwealth of Australia.
38 Australian Digital Health Agency (2017). Australia's National Digital Health Strategy, Commonwealth of Australia.
39 ACS (2017). *Data Sharing Frameworks – Technical White Paper.*
40 Productivity Commission (2017). *Data Availability and Use*, Report No. 82, Commonwealth of Australia, Canberra.

TABLE 1: MTP OPPORTUNITY VALUE CREATION AND CYBER SECURITY CHALLENGES

CUSTOMER (patients, healthcare providers)	COMPANY (MTP companies)	COLLABORATORS (Government, cyber security)
• Increased gathering and sharing of health data from multiple sources to inform improved diagnosis • Patient ownership and access to data to modify behaviours • Reduction in unnecessary procedures, misdiagnosis and ineffective medications • Reduction in the number of diagnostic procedures	• New business model opportunities enabled by improved access to medical data • Improved access to data assists in shortening development cycles for new therapies • Access to better patient metrics and insights for R&D purposes • Possibility of precision products and services with higher demand and margins • Novel products and services based on population health data, including clinical trials	• Improved health budget planning and distribution • Basis for an expedited local regulatory process • Improved utilisation of public health and medical professionals • Shift towards a more effective integrated health system

CYBER SECURITY CHALLENGES

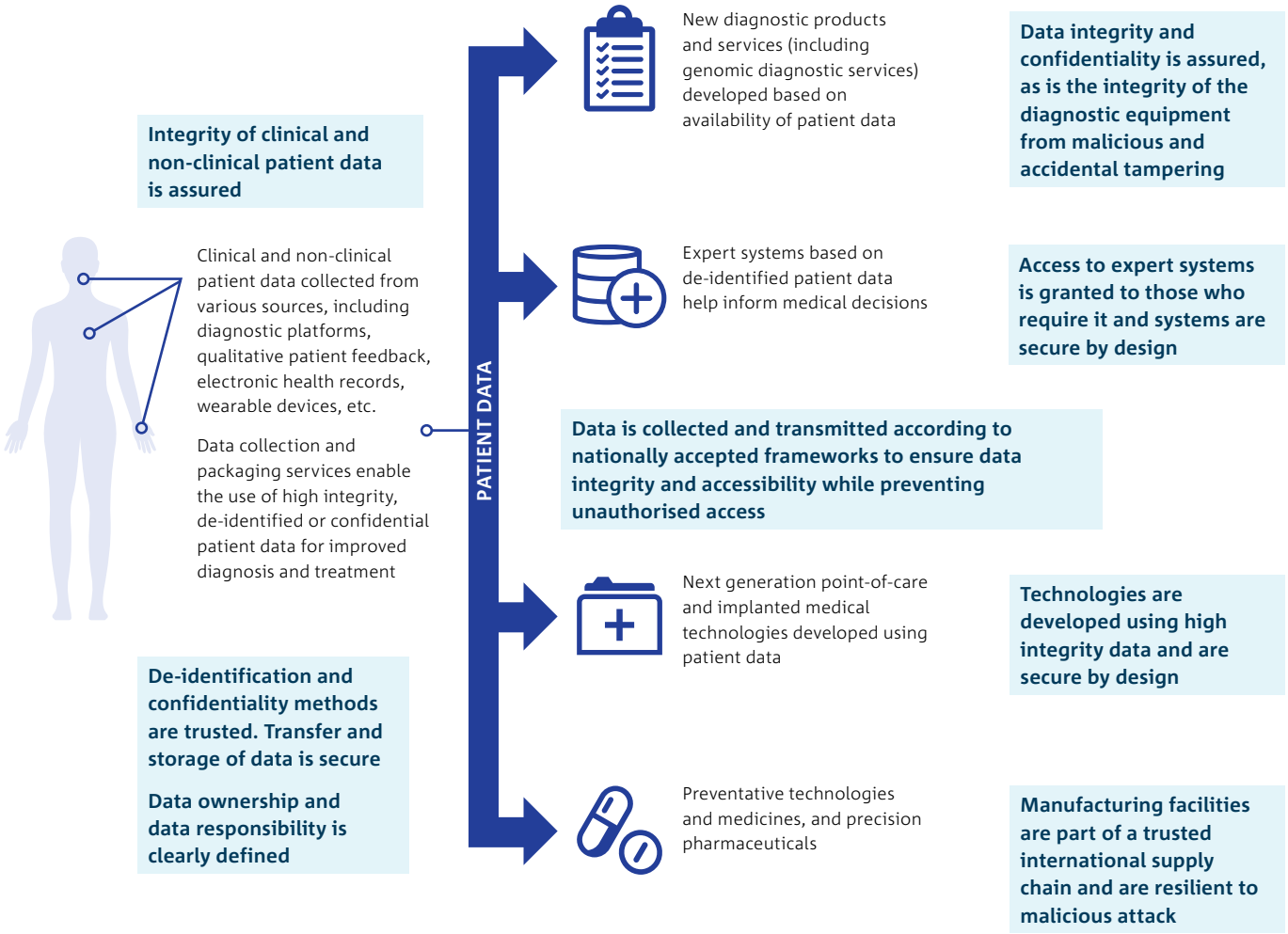
- **Data sharing and access:** Sharing of health data between companies, health providers, researchers and regulators means that clear protection and access control frameworks must be in place to articulate the level of data access, qualify and classify users who can access data, and to ensure organisations can trust the fact that partners are handling data properly. Protection against accidental public data breach and malicious or insider exposure of data is essential. Data must be in a format that is securely sharable and interoperable.
- **Data privacy and ownership**: Assurance of patient privacy and clarity on who owns data is vital when considering current and next-generation health delivery and diagnostic platforms, which are becoming increasingly internet connected and connected with each other. Product and service development will require new paradigms in privacy-preserving analytics to allow sharing of data in ways that ensure it cannot be inappropriately re-identified. This will be supported by building a trusted and federated ecosystem around access to and ownership of this data. Consideration of data ownership is also important where de-identified data is used – for example, in medical research secondary to the original consent, where data could be accurately re-identified by malicious actors.
- **Data integrity:** Completeness and integrity of electronic medical records are sometimes compromised due to inappropriate workarounds, resulting from resistance to changing work practices and patient accessible advanced privacy controls available in My Health Record. Confidence in the integrity of patient health data sources and inputs (including that from wearable devices) needs to be maintained otherwise the data will hold no value.
- **Insider threats:** Employees, contractors or partners wishing to harm a current or former employer, partner or client represent a significant threat to security within a company. Having authorised access means insiders can compromise confidentiality, integrity or availability of networks, data or premises. In the MTP industry, malicious and accidental deletion, alteration, falsification, or unauthorised sharing or public release of patient data is a key challenge.
- **Theft and extortion:** Personal medical data is often a valuable target for theft and extortion, including through cyber means such as phishing and ransomware, both for the business and the patient.

A Ponemon Institute study found that 90% of surveyed healthcare organisations have experienced a data breach in the past two years.[41]

41 Ponemon Institute (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data,* [Online] Available from: https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1 Accessed: 27/02/2018

4.1.2 CYBER SECURE MTP VISION

FIGURE 7: CYBER SECURITY CONSIDERATIONS FOR MTP OPPORTUNITY



14% of pathology tests are ordered due to lack of access to patient's history.[42]

42 Australian Digital Health Agency (2017). *Australia's National Digital Health Strategy, p. 9,* Commonwealth of Australia.

4.1.3 MTP PRIORITY ACTIONS AND R&D

Priority Action 1: Improve healthcare networks and infrastructure

Theme: Secure by design

Fast, cyber resilient networks that allow ubiquitous connectivity within hospitals and healthcare practices are vitally important to enabling improved data transfer and sharing, and allowing implementation of digital technologies to leverage patient data. Consultation for this project indicated that the current state of these networks and their security policies are often restrictive to adoption of advanced digital technologies and patient data sharing.

This is changing as governments begin investing in digital transformation and ensuring an adequate base level of clinical connectivity. For example, the Queensland Government's eHealth Investment Strategy[43] includes an AU $300 million investment into ICT infrastructure, with priorities that include improving the utility of ICT infrastructure and establishing a secure environment to share information and images, as well as consulting with others through an information interoperability platform.

Similarly, the New South Wales eHealth Strategy 2016–2026 identifies improvements to infrastructure, security and intelligence as key focus areas. The NSW strategy aims to develop and enhance minimum standards of infrastructure and network capability, through shifting elements of its infrastructure to 'cloud-based' and 'as-a-service' models.[44]

With the publication of the Digital Hospitals Handbook by Standards Australia[45] and similar digital health infrastructure development initiatives being established across Australian health departments, it is currently a critical time for cohesive cyber security innovation and input.

The MTP and cyber security ecosystem need to:

- Collaborate to ensure infrastructure, network capability and security within healthcare networks are fit for purpose now, and into the future.
- Ensure interoperability of different healthcare networks and infrastructure.
- Develop MTP diagnostics that will efficiently and securely integrate into emerging digital hospital infrastructure including consideration of secure by design principles.

Office of the Australian Information Commissioner (OAIC)

The OAIC has developed business resources and a series of fact sheets concerning the handling of health information for health service providers under the Privacy Act. This resource provides clear descriptions of what constitutes sensitive information, and provides guidelines for health service providers that start to address the challenges concerning patient data sharing and patient privacy. This resource is an important activity towards overcoming the cyber security challenges associated with this opportunity.

Priority Action 2: Develop frameworks for improved clinical data sharing

Theme: Trusted ecosystem

This opportunity leverages the growing quantity and quality of patient data in Australia, and is underpinned by the widespread adoption and expansion of the Australian Government's My Health Record system (electronic health records). Low uptake of this system has triggered its transition to an opt-out participation arrangement which will see a My Health Record created for all healthcare recipients in Australia.[46] As noted in the MTPConnect Sector Competitiveness Plan,[47] if these datasets can be streamlined and securely opened up to the sector for analysis and use in product development, Australia will have a significant advantage across the entire value chain for the development of digitally enabled solutions, and will be much more attractive to international talent, collaboration and investment. As these datasets become

43 Queensland Health (2015). *eHealth Investment Strategy,* State of Queensland, Brisbane.
44 NSW Health (2016). *eHealth Strategy for NSW Health 2016-2026,* NSW Government
45 Standards Australia (2017). *Digital Hospitals Handbook SA HB 163:2017.*
46 Federal Register of Legislation (2017). *My Health Records (National Application) Rules 2017,* Australian Government, [Online] Available from: https://www.legislation.gov.au/Details/F2017L01558/Explanatory%20Statement/Text Accessed: 27/02/2018
47 MTPConnect (2016). *Medtech, Biotechnology and Pharmaceutical Sector Competitiveness Plan.*

deeper and richer, there is a pressing need to ensure their integrity and security against both local and international threats. To enable critical trust in the system, strong privacy, security and risk management frameworks to protect the platform are vital.[48] Building on resources developed by the OAIC, these frameworks need to:

- Protect the confidentiality and integrity of data shared for secondary use through the My Health Record system and other clinical information-sharing platforms.
- Facilitate secure and privacy-preserving messaging and sharing of data between hospitals, health providers and medical technology developers to allow companies to engage in innovative product and service development, using this data as an input.
- Understand how to provide a reliable and consistent operating platform that enables secure availability of information to relevant stakeholders.
- Provide guidance regarding security for remote diagnostics, wearable or implantable medical devices that are capable of transmitting personal data between patients and the clinic.

The cyber security sector and MTP ecosystem need to:

- Engage in the development and adoption of frameworks for clinical data sharing, thereby helping companies in the MTP industry develop processes that ensure privacy and security concerns are addressed, and that innovations are developed in a way that enables data interoperability.
- Advise MTP companies on how best to implement processes that satisfy the requirements of any future data-sharing frameworks, as well as the Privacy Act.
- Coordinate clinical data-handling guidelines with best-practice cyber defences.

Case Study

Australian Genomics Health Alliance

Australian Genomics was launched in 2016 with a National Health and Medical Research Council grant to "*Prepare Australia for the genomics revolution in healthcare*". The collaborative national program is providing evidence to governments for the sustainable, effective and equitable delivery of clinical genomics in healthcare.

Australian Genomics incorporates real-time data and evidence building within clinical projects, and will provide genomic sequencing to over 5,000 Australians by 2020. Intersecting with these clinical projects are programs of work addressing infrastructural challenges to integrating genomics into the health system. This includes supporting cross-cutting development of informatics tools through the diagnostic network; piloting information management requirements and solutions; consulting with Australia's workforce to ensure healthcare providers have the skills and knowledge to effectively deliver genomics; and harnessing an interdisciplinary approach to evaluation, bringing together expertise in implementation science, health economics, bioethics and law to inform health policy and practice.

Cyber security is an essential consideration for Australian Genomics as it investigates frameworks, standards and protocols for the management and sharing of data for clinical care and research. To capitalise fully on the potential of genomic medicine, individual privacy and autonomy must be protected and respected; while data sharing and analysis is critical to advance Australian scientific and medical endeavour. Australian Genomics' *National Data Federation and Analysis Program* is working to balance these needs – with rigorous cyber security policies and protections; data governance and access procedures; and putting the patient in control through a web interface incorporating dynamic consent.[49]

48 Australian Digital Health Agency (2017). *Australia's National Digital Health Strategy,* Commonwealth of Australia.
49 Australian Genomics Health Alliance (2018). [Online] Available from: https://www.australiangenomics.org.au/ Accessed: 28/02/2018

Building on existing initiatives

Australia has initiated the National Digital Health Strategy, which aims to see Australia become a world leader in digital health by leveraging data to deliver new MTP solutions. This supports the opportunity for novel diagnostic and informatics products and services, and will require a strong focus on cyber security to allow consumers and healthcare providers to have trust in digital health applications. The Digital Health Cyber Security Centre aims to protect national digital health systems and personal health information of Australians from cyber threats, and to raise the security posture of the Australian health sector.[50,51] Any actions suggested in this document consider and build on the activities currently underway in the Australian Digital Health Agency, especially frameworks for secondary data use under My Health Record. This will accelerate the development of new MTP platforms and solutions by facilitating secure, trusted data sharing between hospitals, health providers, medical technology developers and consumers.

Future research priorities

Research priorities underpinning these actions include:

- innovation in digital identity management and endpoint authentication
- user-friendly and secure data access and data privacy solutions
- securing data in motion, including data communication routes, encryption of data and secure and privacy-preserving data linkage
- privacy by design in health informatics
- data visualisation and advanced analytics, including privacy-preserving analytics
- advanced security for IoT devices and end points, such as personal wearable and implantable devices, medical equipment etc.
- information interoperability solutions
- advanced threat detection solutions, including artificial intelligence.

Case Study

Curve Tomorrow

Curve Tomorrow is a digital health technology company based in Melbourne, with offices around the world. The company develops technologies and also provides consulting services. Curve Tomorrow's portfolio includes a number of mobile applications, portals, and databases that allow for early detection and diagnosis, decision support, symptom tracking or clinical research. These technologies are used by both patients and clinicians, and rely on secure access, storage and transfer of data between devices, clinical platforms and healthcare environments.

Two examples of Curve Tomorrow technology include: (1) the Q-Max desktop application that rapidly increases clinical efficiency for detecting specific epigenetic mutations that cause Fragile-X syndrome, and (2) the A.L.T. iPad platform that assists clinicians with the identification of speech delay and language issues and is fully integrated into the Murdoch Children's Research Institute (MCRI) research data storage system.[52]

A clear cyber security strategy is critical for the safe deployment of Curve Tomorrow's portfolio. Cyber security needs to be integrated into the design and development process in order to assure patient confidentiality and information availability. As many of the platforms require information collection and sharing across multiple medical and healthcare environments, integration across platforms, networks and infrastructure is critical to the success of Curve Tomorrow technology.

50 Australian Digital Health Agency (2017). Australia's National Digital Health Strategy, Commonwealth of Australia.

51 Australian Digital Health Agency (n.d.). *About the Digital health Cyber Security Centre*, [Online] Available from: https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/about Accessed: 28/02/2018

52 Curve Tomorrow (2018). [Online] Available from: http://www.curvetomorrow.com/ Accessed: 28/02/2018


PERK
01
02
03
04
05
06
07
08
09
10
11

Australia's mining equipment, technology and services (METS) industry

4.2 Australia's mining equipment, technology and services (METS) industry

4.2.1 DATA DRIVEN MINING DECISIONS

The future data-driven mine will optimise mining operations, reduce timeframes for making high-value decisions and optimise response to market demands. Data will be used throughout the mining lifecycle to draw insights and optimise recommendations based on a multiplicity of sensors deployed throughout a mining operation.[53]

There is a long way to go for Australian mining operations to realise the benefits of the terabytes of data currently being generated on a daily basis. Significant roadblocks include siloed operations, unknown data integrity, and poor IT/OT system interoperability and integration.[54] To overcome these obstacles, operational behaviours need to change so that mining data can be fully integrated into decision-making processes.[55] In addition, implications associated with disperse and remote operations need to be addressed.

Australia's METS organisations will play a key role in driving the development and commercialisation of secure digital technologies and cyber-physical systems that can improve the utilisation of data-driven decisions in the mining sector. This includes both the development of information collection devices, such as advanced sensors and other connected, communicative and automated mining equipment and processes; and services to assist mining operators develop platforms to integrate collected data into real-time decision making.

16% of mining businesses in Australia have experienced an internet security incident or breach.[56]

The METS industry is defined as any company that provides specialised products, technologies and services across the mining value chain.[57] This includes companies that provide information and communication technologies and services, including cyber security. The cyber security segment of the METS industry is small; a large proportion of companies (42%) manufacture or distribute mining equipment.[58] To capitalise on the opportunity for data driving mining, these METS companies, in particular, need to consider cyber security as part of their value proposition for their mining company customers. With 66% of Australian METS exporting their products and services,[59] the integration of cyber secure practices into product development represents a global strategic opportunity. Consequently, those companies that are not secure by design are unlikely to build a competitive position in the global market.

Rio Tinto's Mine of the Future project is delivering a 300-400% return on investment.[60]

Australia's mining industry is a target for cybercrime, with motivations based on simple monetary benefits through to gaining information on novel research or technology to erode Australia's competitive advantage; strategic campaigns aimed at weakening Australia's national economy; and environmentally-motivated hacktivism attacks that aim to inflict damage and disrupt business operations.[61] Continuity of operation is essential as a significant disruption not only affects the mining company, but also the supply chain (including METS businesses) with flow-on effects for associated communities and, in extreme cases, affecting Australia's export potential.[62] As such, it is important that mining companies view METS-based cyber security investment as an enabler for sustainable business operation and growth.[63]

53 CSIRO Futures (2017). *Mining Equipment, Technology and Services – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
54 Austmine (n.d.). *The Digital Mine*, [Online] Available from: http://www.austmine.com.au/Publications/the-digital-mine Accessed: 28/02/2018
55 Cann, C. (2017). *Miners should focus on digitisation, says EY*, Mining Magazine.
56 ABS (2017). *8129.0 - Business Use of Information Technology, 2015-16*; 'Table 14: Characteristics of Internet Access, 2015-16' data cube, Canberra.
57 CSIRO Futures (2017). *Mining Equipment, Technology and Services – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
58 CSIRO Futures (2017). *Mining Equipment, Technology and Services – A roadmap for unlocking future growth opportunities for Australia,* Canberra.
59 METS Ignited (2016). *Mining Equipment, Technology and Services – 10 Year Sector Competitiveness Plan (SCP).*
60 Austmine (n.d.). *The Digital Mine*, [Online] Available from: http://www.austmine.com.au/Publications/the-digital-mine Accessed: 28/02/2018
61 Huq, N. (2016). *Cyber Threats to the Mining Industry*, Trend Micro.
62 Gros, R. (2017). Submission to The Senate Standing Committee on Trade and Investment Growth: Inquiry into the Trade System and the Digital Economy, [Online] Available from: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Trade_and_Investment_Growth/Tradeanddigitaleconomy/Submissions Accessed: 28/02/2018
63 Hines, A. (2016) *Cyber security – managing risk amongst disruption,* Mining Journal, [Online] Available from: http://www.mining-journal.com/telstra/partner-content/1173880/cyber-security-%E2%80%93-managing-risk-disruption Accessed: 28/02/2018

TABLE 2: METS OPPORTUNITY VALUE CREATION AND CYBER SECURITY CHALLENGES

CUSTOMER (mining companies)	COMPANY (METS companies)	COLLABORATORS (supply chain, cyber security)
• Savings in time and money, while improving safety and sustainability • Real-time understanding of the impact on the upstream and downstream supply chains • Prevention of costly downtime • Reduced need for reactive maintenance • More transparent operations • Improved understanding and skills associated with cyber secure practices	• Trusted insider access to mining data and insights can open up new opportunities for products and services • New business models focused on provision of secure analytics and real-time insights, together with next-generation digital infrastructure • Trusted engagement with customers • Improved security posture, enhanced protection of IP and knowledge	• Greater demand for robust cyber security solutions • Sharing of trends and insights with partners will allow for greater efficiency in the supply chain • Data insights allow for improved product development cycles for cyber security companies

CYBER SECURITY CHALLENGES

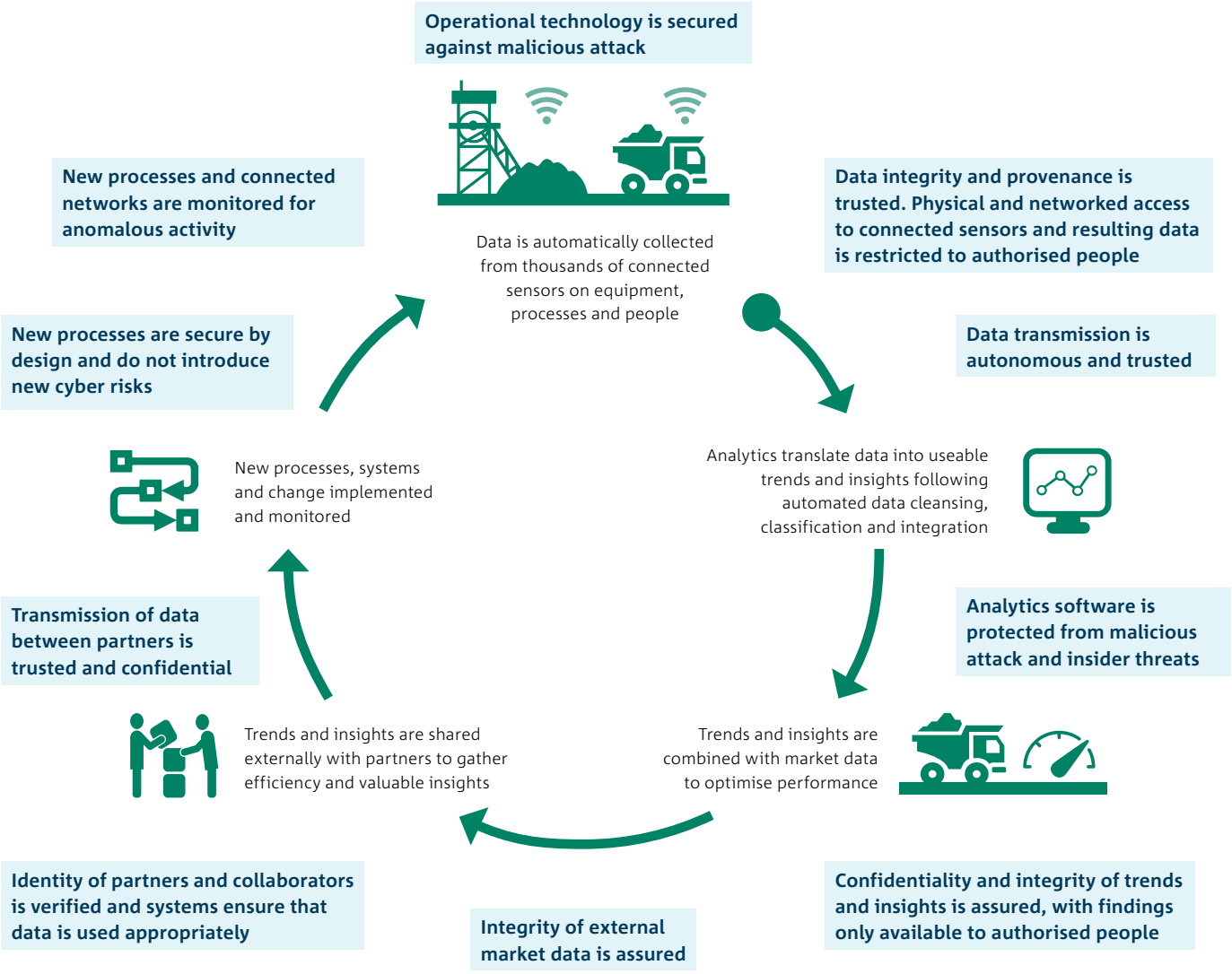
- **Operational technology:** Operational technology (OT) is critical for mining operations; however, these technologies are often legacy systems that are poorly protected from cyber incidents. Many companies have increased spending on corporate IT security. However, the same focus has not been given to OT systems since, when combined with a shortage of skilled cyber security personnel, cyber security threats often go undetected.[64] Attacks on OT can influence the physical world, affecting the continuity of operations and, at an extreme, people's safety.
- **Connected equipment and sensors:** Poor security standardisation and limited baseline security often leave networks of connected mining equipment and sensors vulnerable to attack. As data from these sensors informs mining decisions that result in changes to the environment, security to ensure the integrity of data is vital to ensuring mine safety. Security challenges also arise in relation to the continuity of operations in an environment reliant on information from physically remote equipment and sensors.
- **Availability of data:** The connected mine must ensure operations data and intellectual property is kept secure, accurate and available to those who are authorised to use it. Sharing of mining data throughout the supply chain requires protections and access control frameworks to be in place to articulate the level of data access, qualify and classify users who can access data, and to ensure organisations can trust that partners are handling data properly and not introducing new risk. Protections need to be put in place to ensure against inappropriate use of data.
- **Anomaly detection:** Insights extrapolated from mining data will be used to optimise or instigate new processes or systems. Detecting unauthorised or anomalous activity in new processes, systems or changes is important to ensure that attacks do not go undetected.
- **Volatility of markets:** Mining companies need to respond to the volatility of the supply and demand needs of a market-driven economy by adjusting production accordingly. This has cyber security implications as the integrity and availability of market data becomes more valuable.

Large mine sites in Australia are already generating terabytes of data each day.[65]

64 Deloitte (2017). *Tracking the trends 2017.*
65 Austmine (n.d.). *The Digital Mine*, [Online] Available from: http://www.austmine.com.au/Publications/the-digital-mine Accessed: 28/02/2018

4.2.2 CYBER SECURE METS VISION

FIGURE 8: CYBER SECURITY CONSIDERATIONS FOR METS OPPORTUNITY OPPORTUNITY



4.2.3 METS PRIORITY ACTIONS AND R&D

Priority Action 1: Improve the security across connected mining environments

Theme: Secure by design

Ubiquitous sensing, digitisation and data analytics is a key industry priority for the METS industry, as highlighted by METS Ignited – the METS industry growth centre.[66] It is imperative that networked equipment and sensors that facilitate the collection, analysis and use of mining data for decision making are secure by design. Cyber security companies and research organisations will need to work with Australian METS companies to ensure that security is a consideration in the early stage development of these products and with regards to how they are implemented in mining operations. This will include building cyber security awareness and skills within METS companies, as well as co-development of security for mining equipment, processes and people via an improved user experience. Maximum impact will occur by building on the momentum provided by entities such as Austmine and METS Ignited via their digital mining initiatives, thereby ensuring that METS businesses consider cyber security implications during the development of new METS solutions.

Together, the cyber security sector and the METS ecosystem need to do the following:

- Work with industry associations to create awareness in the METS sector about the enabling role that strong cyber security can play and build domain expertise across cyber security businesses.
- Develop guidelines and solutions to help METS companies integrate appropriate security into new products and equipment (particularly those enabled by sensors) destined for the mining industry, while still drawing out the necessary information required for data driven mining.
- Work with METS companies to test and prove the cyber security claims of new connected technologies and mining equipment, particularly given that the quality and reliability of the outputs for decision-making purposes is key to building confidence in METS solutions within the mining community.
- Assist METS companies in assessing the cyber resilience of their supply chain and companies involved in the cyclical network for data exchange.
- Collaborate with the research and mining sectors to develop new solutions to improve security in mining equipment, and to understand the possible cyber security impacts associated with new communicative technologies such as smart robotics and aerial drones.

Case Study

MICROMINE

MICROMINE, founded in Western Australia in 1986, is an innovative software company with solutions that span the breadth of the mining lifecycle. MICROMINE's software is in use at more than 2,000 mine sites across 90 countries, providing mining companies with solutions to improve the collection and use of data to maximise asset value, increase productivity and help improve data-driven decision making.

MICROMINE's software provides flexible and secure data management solutions, assisting mining companies to access and utilise current operational data, as well as solutions to effectively integrate legacy data from old systems. Understanding that mining operations rely on the security and integrity of data to make informed decisions, the company ensures current best practice for cyber security and data management is adhered to in the development of software.[67]

66 METS Ignited (2016). *Mining Equipment, Technology and Services 10 Year Sector Competitiveness Plan, p. 111.*
67 Micromine (n.d.). [Online] Available from: https://www.micromine.com/ Accessed: 20/03/2018

Priority Action 2: Improve the safe integration of legacy technologies and systems

Theme: Robust and resilient

Historically, operational technology environments have been isolated from other networks, generally with very limited connectivity. Consequently, these legacy systems have very few cyber security safeguards. However, as the desire to integrate and connect systems and extract information from legacy equipment grows, the shortfall in cyber security safeguards presents vulnerabilities. METS-focused cyber services and solutions are improving the safe integration of legacy operational mining technologies with business IT systems.

The cyber security sector needs to:

- Work with METS companies to proactively identify legacy systems that introduce the most cyber security risk when connected to business systems and develop a plan to mitigate this risk when connecting these technologies.
- Help METS companies develop processes to test the safe integration of legacy technologies, such as connected sensor systems.
- Work with the METS industry to leverage the Mining and Metals Information Sharing Analysis Centre (MM-ISAC) to facilitate rapid sharing of critical cyber security information that has an impact on legacy systems.

Future research priorities

Research priorities underpinning these actions include:

- secure and intrinsically safe wireless data communication tools (including low bandwidth communication tools)
- improve latency in data collection between events, decision and action
- secure cognitive computing/artificial intelligence for predictive and pre-emptive analytics
- advanced security for IoT devices and end points, such as personal wearable devices used for improving employee safety, and drones used for data collection and monitoring
- information and system interoperability, security and privacy solutions
- user-friendly and secure data access and federated data analytics to reduce risk of exposing sensitive information
- secure by design embedded intelligent materials
- advanced threat detection solutions, including artificial intelligence and predictive threat detection.

Case Study

RPMGlobal

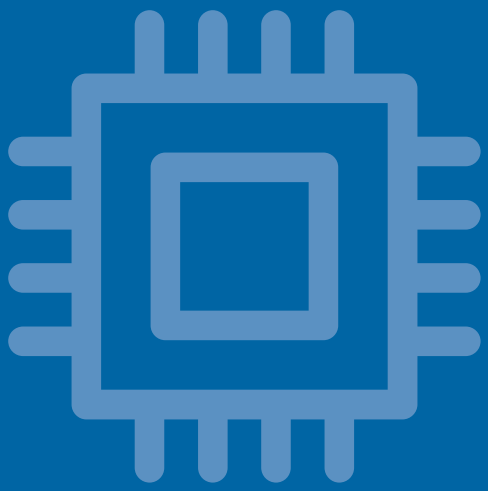
RPMGlobal (RPM) is an Australian-based global company that develops software solutions for the mining industry, including mine planning, simulation, costing, maintenance and execution systems. RPM aims to deliver complete commercial off-the-shelf enterprise platforms for the mining industry, built on open industry standards which deliver a step change in value chain optimisation.[68] This includes creating an advanced Short Interval Control System for mining companies that will assist to improve efficiencies and reduce the cost of mining by enabling real-time performance monitoring of mining equipment.

To do this, data is collected from different equipment and information systems on a mine site in real time through the integration of sensors. This is a complex process, as unscheduled outages, equipment and systems failure and changing work practices affect data output and integrity. Security and integrity of this data is vital, as issues with the data can undermine the reporting process and result in inefficient operating decisions. As such, the company actively works to identify and resolve these issues rapidly to ensure the integrity and continuity of its systems. The company conducts multiple daily system health checks and ensures the integrity of its data through source verification.[69] Cyber security for end points and operating systems is vital to ensuring the integrity and safety of data-driven mining decisions.

68 RPMGlobal (2018). *RPMGlobal announces the completion of the MinVu acquisition*, [Online] Available from: http://www.rpmglobal.com/mediarelease/rpmglobal-announces-the-completion-of-the-minvu-acquisition/ Accessed: 28/02/2018

69 MinVu (n.d.). *Support,* [Online] Available from: https://minvu.com/Support Accessed: 28/02/2018

Australia's advanced manufacturing industry



4.3 Australia's advanced manufacturing industry

4.3.1 CUSTOMISED HIGH-MARGIN SOLUTIONS

Changing demographics, rising incomes and greater customer expectations are driving an opportunity for Australian manufacturers to develop services that provide customised and personalised products which can fetch higher margins. Integrating suppliers and customers into the design and production process can help to develop loyalty and stronger market insights, and hence a greater value proposition.

The value that is generated by advanced manufacturing outputs is apparent within many industries, which makes it an industry horizontal similar to cyber security. This opportunity focuses on customised manufacturing solutions that return value for high-technology industries such as medical technologies, defence and aviation. The opportunity to manufacture customised solutions is driven by a desire for these industries to procure very specific products or components, based on personal information, protected designs or confidential 'one-off' sets of information.

The development of manufacturing services that deliver customised products provides manufacturing businesses with an effective way to supply highly-differentiated solutions that have significantly greater value for their customers. For the foreseeable future, customised high-value manufacturing will allow for larger profit margins across the entire value chain: from research and development to after-sale services and end-of-life management. These solutions are typically delivered in markets where quality factors are valued over cost.

1 in 5 consumers who expressed an interest in personalised products or services are willing to pay a 20% premium.[70]

16% of manufacturing businesses in Australia have experienced an internet security incident or breach.[71]

Success of this opportunity is dependent on manufacturing businesses demonstrating that they can participate in a trusted network and ensure that sensitive data and information (often intellectual property) can be shared via systems that facilitate seamless, rapid and safe exchange with both upstream and downstream members of the supply chain. The integrity of this information needs to be maintained or manufactured products may not be fit for purpose. Information needs to be available to the employees and companies that require it to manufacture products, with confidentiality requirements adequately weighted against accessibility.

Digital technologies will continue to significantly change the way advanced manufacturing businesses operate. Much of this falls under the umbrella of Industry 4.0 – the digitalisation across manufacturing underpinned by automation, machine-to-machine and human-to-machine communication, and artificial intelligence.[72] Industry 4.0 is expected to provide benefits that include accelerated development cycles, and real-time insight into operations allowing increased efficiency and a more complete operational outlook. These are important reasons for improved cyber security in manufacturing businesses.

The most common motivation for cyber-attacks in the manufacturing industry is generally to gain access to intellectual property.[73] Other motivations may include gaining access to sensitive customer data and systems, strategic disruption for competitive and financial advantage, and malicious alteration of product specifications.[74] Australia's advanced manufacturers need to consider how investment in cyber security can enable them to capitalise on the opportunity to create customised solutions for end users.

70 Deloitte (2015). *The Deloitte Consumer Review – Made to Order: The rise of mass personalisation*, London.

71 ABS (2017). *8129.0 - Business Use of Information Technology, 2015-16*; 'Table 14: Characteristics of Internet Access, 2015-16' data cube, Canberra.

72 Department of Industry, Innovation and Science (2017). *Industry 4.0,* [Online] Available from: https://industry.gov.au/industry/Industry-4-0/Pages/default.aspx Accessed: 27/02/2018

73 Deloitte (2016). *Cyber risk in advanced manufacturing,* Manufacturers Alliance for Productivity and Innovation (MAPI).

74 Deloitte (n.d.). *Global Cyber Executive Briefing Manufacturing,* [Online] Available from: https://www2.deloitte.com/global/en/pages/risk/articles/Manufacturing.html Accessed:28/02/2018

TABLE 3: ADVANCED MANUFACTURING OPPORTUNITY VALUE CREATION AND CYBER SECURITY CHALLENGES

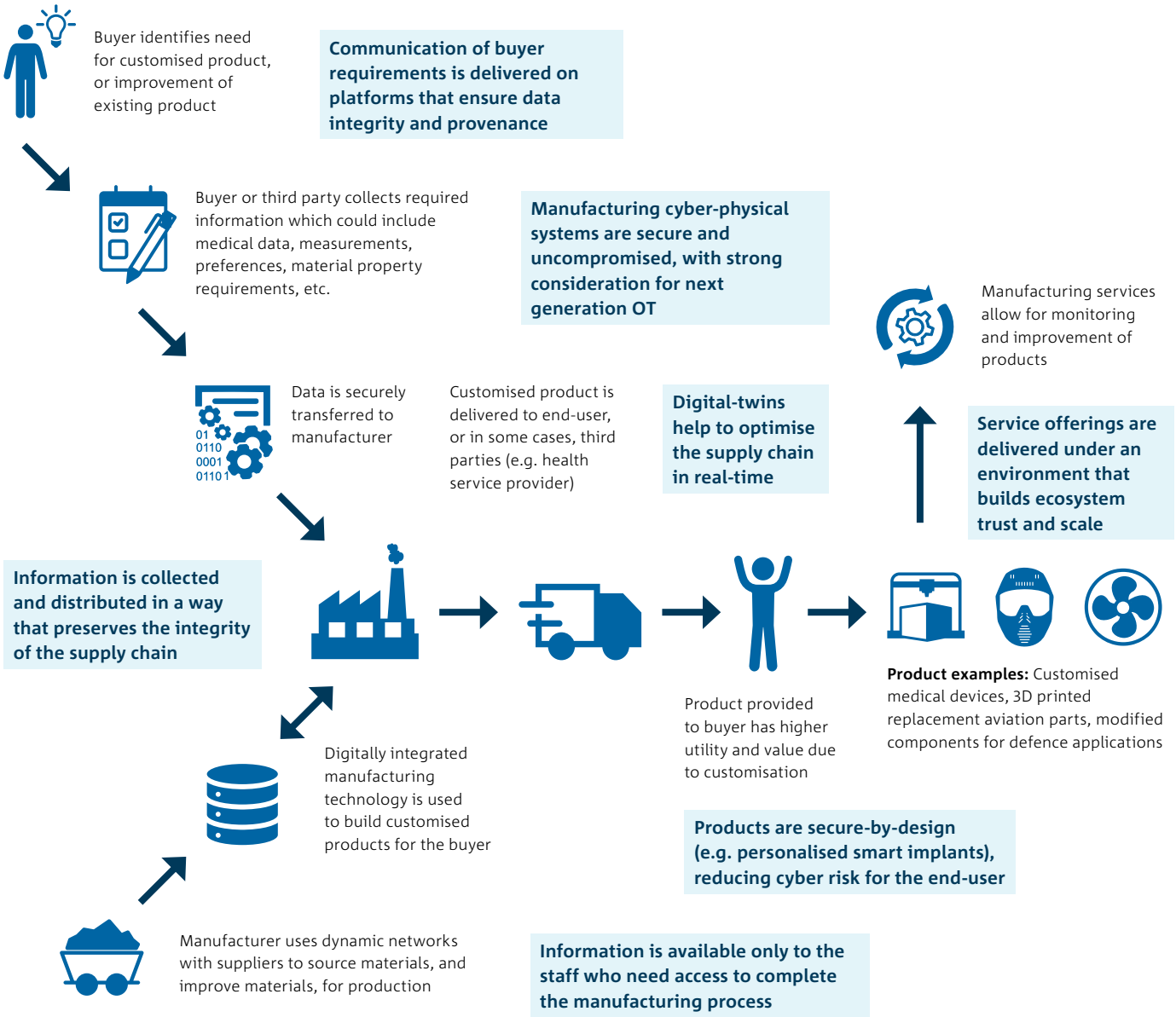
CUSTOMER (end consumers, supply chain)	COMPANY (advanced manufacturing companies)	COLLABORATORS (supply chain, cyber security)
• Customer's needs are met, leading to improved satisfaction • Greater variety in product specifications, including materials • Customers may have enhanced experiences when engaged in creation and design of their own products • Streamlined process facilitated by online customised ordering and payment	• Customer's willingness to pay increases manufacturers' ability to charge a higher margin • More meaningful engagement builds loyalty • Introduction of novel manufacturing processes, equipment, materials and value chains • Collection of more details/data from customers in the ordering process can provide unique insights for improved or entirely new products and services • Greater potential for add-on product or services	• Increased demand for new and diversified supply chain partners • Increased demand for novel materials and inputs • Collection of personal data will create demand for cyber security • Growing demand for 'smart' products will drive collaboration

CYBER SECURITY CHALLENGES

- **Security confidence:** Many of the industries that will benefit from customised manufactured solutions, such as medical technologies, aviation and defence, need to feel confident that their sensitive information, technologies and intellectual property will remain within the confines of trusted parties.
- **Insider threats:** Employees and trusted partners pose significant challenges to the safe custody of data in manufacturing. Insiders can cause malicious and accidental alteration, falsification, or unauthorised sharing or public release of client's intellectual property or personal information.
- **Supply chain integrity:** Manufacturing ecosystems are complex; often involving dozens of participants and sources of data and information in the supply chain from raw materials through to the end user. This complexity provides a malicious actor with an increased range of likely human- and machine-related vulnerabilities that can be exploited. Customised manufacturing will require that the supply chain remains intact, as disruptions of any kind will have a significant impact on a company's ability to deliver to the end user.
- **Data integrity:** In order for customised solutions to maintain value, they must be delivered to the exact specifications of the end user. Failure to achieve this could deliver an unusable component or even a life-threatening product.
- **Data availability:** To effectively build relationships with up and downstream supply chain partners, data flow must be dynamic, thereby allowing for optimisation of the manufactured solution. The ability to securely and rapidly share data will improve development cycles and potentially decrease costs.
- **Connected equipment:** Manufacturing processes and equipment are progressively being controlled via Industry 4.0 technologies (automation, sensors etc.), which increases the company's reliance on third party equipment and networked solutions, and introduces cyber security risks. Since connected equipment and devices are primary sources of data and are often insecure by design, they are important targets for malicious activity.

4.3.2 CYBER SECURE ADVANCED MANUFACTURING VISION

FIGURE 9: CYBER SECURITY CONSIDERATIONS FOR ADVANCED MANUFACTURING OPPORTUNITY



4.3.3 ADVANCED MANUFACTURING PRIORITY ACTIONS AND R&D

Priority Action 1: Improve channels for supply chain data sharing

Theme: Trusted ecosystem

As companies seek to develop business around the provision of customised products and services, their ability to transmit, receive, store and utilise data securely is critical, and their processes for doing this will be scrutinised by potential clients and supply chains. A major problem these clients and supply chains grapple with is concern about the appropriate level of information they should share with manufacturers in order to balance their ability to do a good job with the protection of their intellectual property. Because of this, manufacturing companies must demonstrate that their data handling practices will protect the intellectual property and proprietary information they receive from their clients and supply chains, and that they have safeguards in place to prevent their systems from being breached.

The manufacturing and cyber security sectors need to:

- Collaborate to design and develop robust data handling procedures and systems to ensure the confidentiality of shared client data. These procedures will be important in building trust and confidence, thus allowing clients to feel comfortable sharing their data with manufacturers. This data may be detailed specifications and intellectual property from organisations, or personally identifiable information provided by individuals.
- Establish protocols for allowing transparency for appropriate information while maintaining confidentiality of other information in a digital supply chain.
- Develop best practice risk-benefit analyses to understand the appropriate level of data sharing within supply chains and establish suitable control mechanisms and data-sharing policies.

Case Study

Anatomics

Anatomics Pty Ltd – an Australian medical device company that specialises in the design and manufacture of patient-specific implants – demonstrates the growing importance of customisation in medical technology manufacturing. Founded in 1996, Anatomics has pioneered the use of medical imaging to develop personalised surgical implants that utilise innovative and advanced manufacturing techniques such as 3D printing, thus saving time in the operating theatre and enabling better patient outcomes. The range of customised implants Anatomics manufactures allows surgeons to consider undertaking a whole new suite of operations that were once impossible. Implants are manufactured from a range of materials, including acrylic, titanium and porous polyethylene.

As a result of its customised implants, Anatomics has helped over 4,000 patients. For example, in a world first surgery, Anatomics designed and manufactured 3D-printed vertebrae to replace two cancerous vertebrae from a patient's neck, allowing anatomically correct replacement for better outcomes.

Anatomics is integrating distributed manufacturing into hospitals and uses an integrated software platform to provide healthcare professionals with access to patient data to formulate specific therapeutic strategies for their patients. The platform shares information with all healthcare stakeholders to encourage innovative problem solving. Efficient information sharing is important for Anatomics' business model, both with customers through the software platforms and with supply chain partners. Secure information sharing through software platforms is enabled by robust security and privacy practices that protect sensitive information and creates trust in the platform.[75]

75 AnatomicsRX (n.d.). *Privacy,* [Online] Available from: https://www.anatomicsrx.com/Privacy Accessed: 28/02/2018

Priority Action 2: Ensure secure integration of cyber-physical manufacturing systems

Theme: Secure by design

New cyber-physical manufacturing systems are allowing companies to use intelligent machines, networks and systems that independently communicate and co-operate with each other over the entire manufacturing floor. These systems can help improve manufacturers' competitiveness by enabling rapid and/or customised design and production solutions for clients through connected technologies such as automation, robotics and 3D printing. Advanced cyber-physical manufacturing systems will also enable manufacturing business model innovation, with opportunities to focus on servitisation supported by improved data collection.

To remain globally competitive, Australian manufacturing companies need to consider cyber-physical manufacturing technologies and embed practices that will allow for their secure integration and reduce vulnerability to potential cyber security disruptions.

Success of this manufacturing approach requires strong cyber security protections. It is important that new cyber-physical manufacturing platforms are secure by design, as well as any integrated components from global supply chains. In an environment with extensive dynamic connectivity, cyber-attacks can have highly damaging implications, both for the manufacturing company and the broader supply chain.

Together, the manufacturing and cyber security sectors need to:

- Build awareness in manufacturing companies about the importance of cyber security, especially as they adopt new technologies and engage in new supply chains.
- Develop digital twins to collect information in real-time and allow for extensive and secure testing of the manufacturing system's agility and response.[76]
- Develop cyber security strategies for improved resilience, detection, response and recovery in the manufacturing industry by moving security measures from reactive to proactive. This will include strategies to establish minimum security requirements for vendors and suppliers.

Future research priorities

Research priorities underpinning the growth of this sector include:

- cloud-based security and privacy solutions for connected manufacturing equipment
- real-time vulnerability, anomalous activity and intrusion detection for manufacturing systems, including IoT devices
- advanced security for additive manufacturing product development software systems
- effective platforms that manage the provenance and integrity of Intellectual Property
- security design innovation for industrial and process control software and systems
- device layer security innovation
- secure communication protocols for data transfer across networks
- scalability of security solutions for an increasingly large number of devices connected to networks.

The Internet of Things Alliance Australia (IoTAA)

The IoTAA was established in 2016 to help empower industry to grow Australia's competitive advantage through accelerated innovation and adoption of the Internet of Things.

Working collaboratively with its 400+ member organisations across key sectors of the Australian economy, the IoTAA promotes and develops the Australian IoT opportunity. It does this through its many workstreams which address different enablers and inhibitors for IoT technologies. One important enabler is cyber security, which is addressed through the IoTAA's cyber security and network resilience workstream. For manufacturers in Australia, the organisation's newly formed manufacturing workstream will focus on accelerating innovation in IoT and cyber security for manufacturers.

76 Parrott, A., Warshaw, L. (2017). *Industry 4.0 and the digital twin,* Deloitte University Press.

Case Study

Tonsley Manufacturing Innovation Hub[77]

Australia has numerous companies that focus on high-value solutions for a variety of industries, including aerospace, aviation, defence, medical technologies, automobile and transport. However, few manufacturers have demonstrated the application of advanced cyber-physical production systems and only 2% of Australian business leaders are confident that they can harness the power of Industry 4.0.[78] This has led to the creation of hubs focusing on connecting Industry 4.0 researchers with practical commercial outcomes in an effort to shift Australian manufacturers towards platforms that result in more competitive manufacturing processes.

The Tonsley Manufacturing Innovation Hub (TMI), located within the Tonsley Innovation Precinct in South Australia, is one example. Working closely with the Innovative Manufacturing Cooperative Research Centres (CRC), the TMI aims to accelerate the adoption of advanced digital technologies and automation in manufacturing businesses, and plays a catalytic role in promoting understanding and application of Industry 4.0.

At the heart of the TMI is the Factory of the Future – an education, training and research facility that showcases the latest in cyber-physical, automation and robotic technologies. This facility and the training it provides assist manufacturers to integrate technologies and business models that are changing the way they connect with customers and suppliers through digital internet-based technologies. The ability to securely integrate and adopt advanced cyber-physical systems is important for the competitiveness of Australian manufacturers and requires an early and thorough understanding of cyber security requirements and solutions.

The Australian Government is actively supporting the development of Australia's advanced manufacturing industry for defence products, including through the Defence Export Strategy.[79]

77 Australian Manufacturing (2018). *World-class advanced manufacturing hub opens in Tonsley,* [Online] Available from: http://www.australianmanufacturing.com.au/50091/world-class-advanced-manufacturing-hub-opens-in-tonsley Accessed: 28/02/2018

78 Deloitte Insights (2018). *The Fourth Industrial Revolution is here— are you ready?*

79 Department of Defence (n.d.). *Defence export strategy – Fact sheet*, Australian Government.

Australia's oil and gas industry

4.4 Australia's oil and gas industry

4.4.1 DIGITAL OPERATIONS AND MAINTENANCE

Rapidly evolving digital technologies provide an opportunity to transform exploration, production, inspection and maintenance activities across onshore and offshore Australian oil and gas developments. In particular, technologies such as artificial intelligence (AI), automation, virtual reality and digital twins will help to improve the safety and efficiency of operations and maintenance at Australia's remote sites by enabling remote and autonomous operations.

Australian liquefied natural gas (LNG) operations and maintenance annual expenditure is expected to increase from AU$1.3 billion in 2014 to AU$4.9 billion by 2020.[80]

The potential for the Australian oil and gas industry to capitalise on these digital technologies is significant and is driven by the need for improved efficiencies due to sustained low oil prices and the industry's growing operational expenditures. Although digital technologies are not new to the oil and gas sector, the full potential of these technologies has not yet being realised which presents valuable opportunities for growth. However, these opportunities could be easily undermined, especially if the industry's pursuit of interconnectedness outpaces its cyber maturity.

Digital solutions that are particularly valuable are those that enable the remote operation and maintenance of facilities, such as robotics and unmanned vehicles for activities such as drilling and inspection and Remote Operation Centres (ROCs). These technologies are well suited to help streamline operations and address safety issues associated with the sector's general remoteness (both for offshore and onshore resources). Data collection and analysis will also help to optimise operations and supply chains. For example, big data analytics and AI can be applied to more efficiently match supply with demand,[81] while blockchain technology may be employed to streamline contracts and payments to gain further efficiencies.[82]

Australia's oil and gas sector, as part of a highly globalised industry, relies heavily on a network of global service companies to generate a large proportion of the industry's innovations, including digital technologies. The requirement for a robust cyber security strategy needs to be addressed by organisations in the oil and gas industry, but also within these service companies when developing solutions for the industry.

As Australia's oil and gas industry is generally considered to be part of Australia's critical infrastructure, disruptions to operations caused by cyber-attacks could have serious implications for Australian business, government and the community. With over half of all Australian-produced gas destined for export markets,[83] the industry is also critical to the energy security of many countries globally.

Similar to the METS and mining industry, oil and gas companies are vulnerable economic and geopolitical targets for cybercrime, with potential motivations extending beyond monetary gain to eroding Australia's competitive advantage, weakening the national economy, environmentally-motivated hacktivism and terrorism. These motivations – together with the industry's complex ecosystem of computation, networking, automation and geographic spread – make it a vulnerable target that would gain value from innovative cyber security solutions.

A global EY survey found that 60% of oil and gas organisations have experienced a recent significant cybersecurity incident.[84]

80 Accenture (2015). *Ready or Not? Creating a world-leading oil and gas industry in Australia.*

81 Booth, A., Mohr, N., Peters, P. (2016). *The digital utility: new opportunities and challenges,* McKinsey & Company, [Online] Available from: http://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/the-digital-utility-new-opportunities-and-challenges Accessed: 28/02/2018

82 World Economic Forum (2017). *Digital Transformation Initiative: Oil and Gas Industry*, Geneva.

83 National Energy Resources Australia (2017). *Sector Competitiveness Plan,* Kensington.

84 EY (2017). *Cybersecurity regained: preparing to face cyber attacks, EY 20th Global Information Security Survey 2017–18 Oil and gas sector results.*

TABLE 4: OIL AND GAS OPPORTUNITY VALUE CREATION AND CYBER SECURITY CHALLENGES

CUSTOMER (end consumers, supply chain)	COMPANY (Oil and gas companies)	COLLABORATORS (cyber security, research)
• Supply chain optimisation improving carriage of data to downstream customers • Improved efficiencies for the company results in improved energy security for the nation (and globally)	• Improved workforce safety, especially in remote environments • Cost efficiencies through improved productivity • Reliable prediction in relation to equipment and process failures allows predictive maintenance, thus eliminating unplanned costly down time	• Digital supply chain optimisation enables seamless communication of production, operational and logistical data • Improved value proposition for industry joint ventures and new Greenfield projects • Digital operations and maintenance will stimulate demand for robust cyber security solutions

CYBER SECURITY CHALLENGES

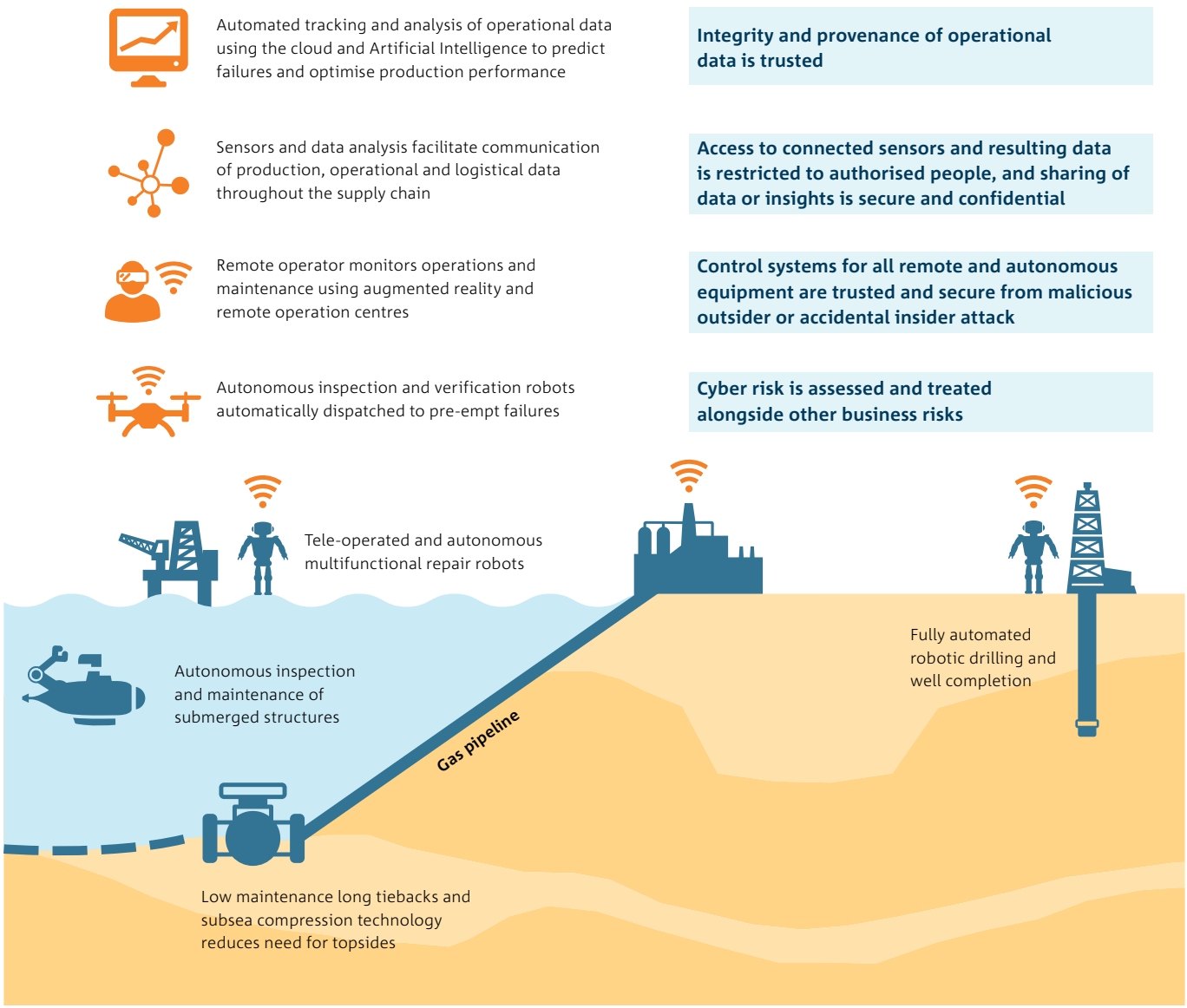
- **Legacy assets:** Upstream production of oil and gas often utilises legacy assets that were not built with cyber security in mind but, rather, have been retrofitted to connect to networks. Connecting these assets has cyber security implications for oil and gas companies.
- **Control and availability of OT:** OT in the digital oilfield must prioritise the requirements for control and availability over integrity and confidentiality. It is vital to protect control and availability as loss of these will have an impact on people's safety.
- **Security of networks:** With sensors deployed across upstream oil and gas operations, it is vital that the network that connects this equipment is resilient to attack. With data from sensors potentially resulting in physical changes to the real-world environment, network security to ensure integrity of collected data is vital to ensuring safety.
- **Physical security:** Securing the industry's physical infrastructure is an important consideration, especially for the onshore industry, where assets are often remote and unstaffed. Cutting fibre-optic cables or theft of drones, for example, will have negative consequences on productivity and safety.
- **Data sharing:** Sharing of production data along the supply chain requires protections and access control frameworks to be in place to articulate the level of data access, qualify and classify users who can access data, and ensure organisations can trust that partners are handling data properly and not introducing new risk.
- **Intelligence sharing:** The critical importance of oil and gas infrastructure has made some governments unwilling to share threat information that is of relevance to the industry. Shared intelligence on credible threats is imperative to good cyber hygiene by helping companies to anticipate breaches and respond quickly. Global sharing of this intelligence needs to be incentivised and encouraged.
- **Data integrity:** Trust in collected data is a challenge to its utility in the oil and gas industry. Data originating for various sources and with different degrees of quality erode the trust operators place in this material. To exploit the full potential of data in this sector, its integrity and quality needs to be monitored and assured.

Estimates show that operators are using less than 1% of the data being captured at the well.[85]

85 Womack, D., et al (2016). *Exploring the power of cognitive IoT,* IBM Corporation

4.4.2 CYBER SECURE OIL AND GAS VISION

FIGURE 10: CYBER SECURITY CONSIDERATIONS FOR O&G OPPORTUNITY



4.4.3 OIL AND GAS PRIORITY ACTIONS AND R&D

Priority Action 1: Improve national and global intelligence sharing

Theme: Trusted ecosystem

In a globalised industry such as oil and gas, sharing of intelligence about cyber threats and other security threats is vital. Developing trusted relationships with foreign companies and governments is important for intelligence sharing. Having early warning about credible threats that face the industry or that have affected similar companies in other nations can allow Australian operations to prepare and improve their defences, and can improve detection and response time.

The oil, gas and cyber security ecosystem need to:

- Encourage the local sharing of threat intelligence and information between oil and gas businesses. This could be done by bolstering the uptake, activity and security of the Australian Government's Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience – in particular, the sharing of cyber security threats and intelligence in the Energy Sector Group and the Oil and Gas Security Forum (OGSF).
- Work with oil and gas companies to help establish access and presence in global intelligence-sharing networks specific to the industry to receive real-time intelligence on credible threats.
- Develop methods to identify credible threats for oil and gas operators from shared intelligence, and a process for addressing and responding to these in a timely fashion.

Case Study

SC8[86]

SC8 is an Australian cyber security company which assists businesses across oil and gas, mining, infrastructure and other markets to improve the resilience and integration of their operational technologies (OT).

The company's proprietary platform combines real-time visibility of connected operational technologies with industry and sector-specific intelligence to provide 'actionable intelligence' for clients. The platform also provides pattern recognition against normal and abnormal behaviour, underpinned by an intrusion detection system.

By providing real-time and shared platform intelligence, SC8 helps companies to not only identify and locate threats in the OT environment, but also to determine their impact on systems and prioritise these against the company's cyber security risk framework and policies, and to inform the response strategy.

Unplanned outages cost the LNG industry approximately US$11 million per day.[87]

86 SC8 (2017). [Online] Available from: www.sc8.com.au/ Accessed: 08/03/2018

87 Thomas, K (2016). *Digitisation decisive in cutting LNG project costs, says GE's Simonelli*, LNG World Shipping, [Online] Available from: http://www.lngworldshipping.com/news/view,digitisation-decisive-in-cutting-lng-project-costs-says-ges-simonelli_42573.htm Accessed 26/06/2017

Priority Action 2: Implement active education programs

Theme: Robust and resilient

Improving industry's ability to quickly and appropriately detect, respond and recover from a cyber security attack is vital. Alongside building greater cyber security awareness and training in the oil and gas workforce, the gap in developing appropriate security for industrial control systems needs to be bridged. Immersive scenario-based education allows organisations to put into practice their cyber security plans, iron out any potential issues, and gain a greater understanding of what needs to be done.

The cyber security sector needs to:

- Work with oil and gas companies to plan and enact active education programs to develop a practiced response to credible cyber security threats.
- Collaborate with industry associations to foster greater awareness of cyber security within oil and gas companies, and greater domain knowledge for cyber security companies.
- Help to bridge the gap in developing appropriate skills for managing security for industrial control systems within the oil and gas sector.

Future research priorities

Research priorities underpinning these actions include:

- secure and intrinsically safe wireless data communication tools (including low bandwidth communication tools)
- secure cognitive computing/AI for predictive and pre-emptive analytics
- greater resilience in industry control systems
- provable trustworthiness of systems used in critical infrastructure
- advanced threat detection solutions, including AI and predictive threat detection
- unknown vulnerabilities, anomalous activity and intrusion detection
- secure by design digital technologies, including 3D printing and inspection technologies (e.g. drones and other unmanned vehicles).

Case Study

RIoT Solutions[88]

Brisbane-based company RIoT Solutions offers a range of cyber security services that cover a wide spectrum of digital technology implementations within enterprise (IT) and industrial control (OT) environments, including specialist areas such as IoT (Internet of Things), IIoT (Industrial IoT), and ICS (Industrial Control Systems).

RIoT Solutions offers cyber security attack simulation services in order to help to better prepare companies for cyber-attacks and to improve resilience. Working with clients, RIoT Solutions tailors simulations to the unique characteristics of the target environment. The simulation service emulates a real-world threat to the organisation, allowing hands-on incident response to help companies identify security weaknesses and areas of improvement, and to test abilities to identify, respond and protect the business from a real-world cyber-attack. These exercises also enable staff to familiarise themselves with their roles, responsibilities and available tools.

In recent cases, RIoT has been able to help clients identify various vulnerabilities that were exploited in the simulation. With data collected from the exercise, clients are able to improve their security protection, as well as improve staff awareness of cyber security threats.

88 RIoT Solutions (n.d.). [Online] Available from: https://www.riotsolutions.com.au/ Accessed: 28/02/2018

Australia's food and agribusiness industry

4.5 Australia's food and agribusiness industry

4.5.1 PREMIUM INTERACTIONS

The growing global middle class and maturing consumer preferences are driving the opportunity for Australia's food and agribusiness industry to develop and export premium products with quality and luxury status, or novel attributes. Providing accurate reporting of food provenance to consumers and businesses in the value chain can enhance the value of exports, and can act as an important differentiator in overseas markets where product attributes such as 'Brand Australia', allergen management and food safety have an impact on buying decisions.

To extract maximum value from premium foods, especially in export markets with complex and multi-point supply chains, Australian businesses will need to investigate technologies to combat food fraud, and improve traceability and authentication of provenance claims.

In 2017, food and wine fraud cost Australian exporters an estimated AU$1.7 billion,[89] thereby threatening Australia's reputation as a high-quality exporter. Food fraud is a broad term which encompasses the deliberate substitution, addition, tampering, or misrepresentation of food, ingredients, or packaging; or false or misleading statements made about a product, such as origin, for economic gain. Food fraud can result in severe public health vulnerabilities such as illnesses and fatalities attributed to inferior product substitution.[90]

Trust in food products is a critical factor for success in export markets, with responsive traceability systems likely to become a compulsory requirement for importing countries in the future.[91] These systems will be supported by accessible and accurate information regarding product and ingredient origin, food processing and distribution details. Access to this information increases consumer confidence in food safety; helping to build high-quality premium brands and improve supply chain efficiency.

Traceability systems can also help to remove fraudulent suppliers from the market. If trust in provenance claims and information chains is destroyed, the reputation of Australian food and produce in export markets will be tarnished. This, in turn, will diminish the value of these markets to Australian industry. Australia has implemented strong identification and traceability systems for livestock (the National Livestock Identification System and PigPass); however, more work needs to done to develop more advanced systems for other export-focused products.

New Australian food labelling requirements come into effect in 2018[92] . These requirements mean that Australian businesses will have to invest in both digital and physical technologies that provide greater transparency around product origin, production inputs, suppliers, processing materials, transport and distribution.[93] These systems will collect, curate and store vast quantities of data, which will increase over time with the use of more automation and robotic technologies in the food and agribusiness industry.

Traceability systems will add value to Australian food products, especially for export markets. The data collected and the infrastructure required to enable appropriate availability of data for these traceability systems will be facilitated by strong cyber security solutions.

Olive oil is often substituted or mislabelled, and is the food most vulnerable to fraud on a global basis.[94]

89 McLeod, R. (2017). *Counting the Cost: Lost Australian food and wine export sales due to fraud.* Food Innovation Australia Ltd.
90 Spink, J. and Moyer, D.C. (2011). *Defining the public health threat of food fraud*, Journal of Food Science 76: 157-163.
91 Commonwealth of Australia (2015). *Agricultural Competitiveness White Paper,* p. 5.
92 Commonwealth of Australia (2016). *Australia's food labels are getting clearer,* [Online] Available from: http://www.foodlabels.industry.gov.au/ Accessed: 28/02/2018
93 CSIRO Futures (2017). *Food and Agribusiness – A roadmap for unlocking value-adding growth opportunities for Australia,* Canberra.
94 Curll, J. (2015). *The significance of food fraud in Australia,* Thomson Reuters.

TABLE 5: FOOD AND AGRIBUSINESS OPPORTUNITY VALUE CREATION AND CYBER SECURITY CHALLENGES

CUSTOMER (consumer, restaurants, retailers)	COMPANY (Food and agribusiness companies)	COLLABORATORS (supply chain, cyber security)
• Assured provenance means consumers get what they have paid for, and increases trust in suppliers and brands • Assurance of ingredient quality and free-from claims lead to trusted product safety for consumers • Qualified provenance claims allows retailers and restaurants to leverage value of brand (e.g. Brand Australia)	• Preserve premiums that producers are able to charge based on an item being a premium product • Reduce food fraud in target markets • Gain a competitive advantage and trusted reputation for commodity foods stuffs • Add-on services around consumer accessible verification of provenance and claims	• Assurance of supply chain product information integrity • The digital verification of provenance and quality of food and beverage products will stimulate demand for robust protection solutions from cyber threats • Paddock-to-plate assurance leads to more trusted suppliers and brands, creating loyalty with consumers and markets

CYBER SECURITY CHALLENGES

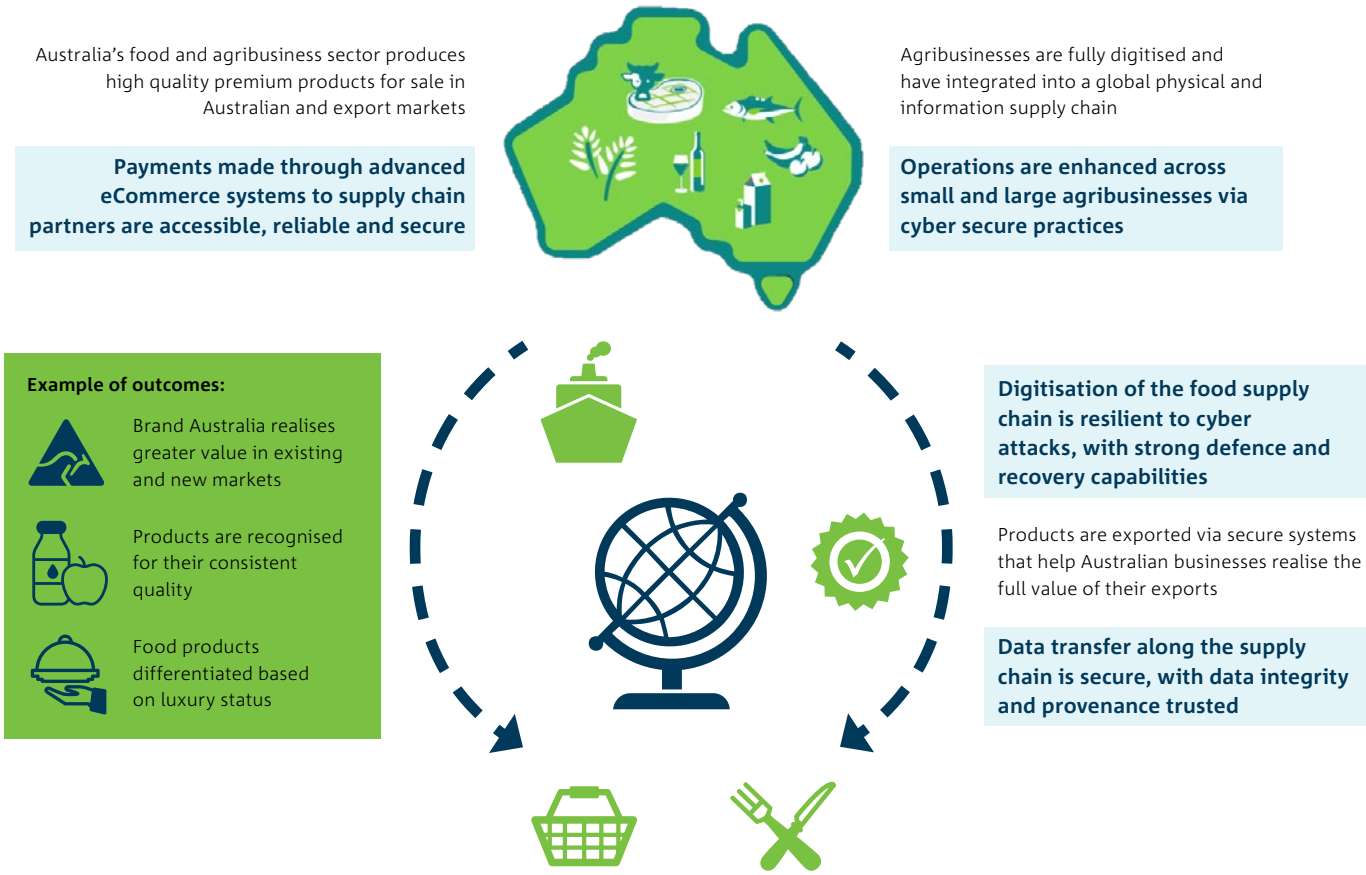
- **Digital maturity**: The digital maturity of Australia's agricultural sector is described as 'ad hoc', meaning it does not systematically and consistently use data to drive decisions.[95] Low digital maturity impedes digital transformation and decreases the competitiveness of the sector, and subsequently presents cyber security risks.
- **Security of sensors:** With sensors deployed across the value chain to monitor quality and movement of food products, it will be vital that the associated networks of connected equipment are resilient to malicious attack. Falsified or incorrect data collected from sensors could lead to food fraud, which will erode markets and potentially have a negative impact on human health.
- **Data sharing:** Sharing of product origin, production inputs, suppliers, processing materials, transport and production data along the supply chain requires protections and access control frameworks to be in place to both articulate the level of data access, qualify and classify users who can access data, and ensure organisations can trust that partners are handling data properly and not introducing new risk.
- **Availability and authentication of provenance data:** With increasing consumer interest in food provenance and transparency, publicly available high-integrity information systems need to be able to provide consumers with information about provenance claims. Authentication of this information is a challenge.
- **Food supply chain security:** The food and agribusiness industry and its supply chain are recognised as important critical infrastructure in Australia, providing essential services for everyday life. Digital transformation and the growing complexity of the industry's supply chains increases the industry's vulnerability to cyber-attack, industrial espionage by cyber means and other sources of system breakdown, which were previously not inherent risks.[96] Such attacks have the potential to have a rapid and widespread impact on a community by not only affecting supply, but also the safety of that supply which can lead to deaths as a result of food becoming biohazardous.

95 Leonard, E., Rainbow, R., Trindall, J., *et al.* (2017). *Accelerating precision agriculture to decision agriculture: Enabling digital agriculture in Australia,* Cotton Research and Development Corporation, Australia.

96 Department of Agriculture, Fisheries and Forestry (2011). *Resilience in the Australian food supply chain, p. vii.* Commonwealth of Australia.

4.5.2 CYBER SECURE FOOD AND AGRIBUSINESS VISION

FIGURE 11: CYBER SECURITY CONSIDERATIONS FOR FOOD AND AGRIBUSINESS OPPORTUNITY



4.5.3 FOOD AND AGRIBUSINESS PRIORITY ACTIONS AND R&D

Priority Action 1: Build awareness of cyber solutions

Theme: Robust and resilient

Digital uptake in Australia's agribusiness industry is slow. As new digital technologies are adopted within the food and agribusiness industry, awareness of cyber security practices needs to be increased. Cyber security products and services need to be marketed in an informative way to businesses looking to implement digital technologies into their operations.

The cyber security sector can assist the food and agribusiness industry by doing the following:

- Develop food and agribusiness specific information and marketing resources, including detailing how specific cyber security solutions may help businesses to become more resilient and to adopt new technologies to pursue digital opportunities. Improving knowledge about available cyber security solutions may help companies in the industry feel more comfortable to participate in a data-driven world.
- Work with companies and industry associations to develop domain expertise and an in-depth understanding of the challenges facing food and agribusinesses in order to develop tailored products and solutions.
- Work with industry associations to raise awareness of cyber security threats and safe computing practices within the industry.
- Assist food and agribusinesses to embed security into business practices and new product development, and help to mitigate legacy system risk as basic digital systems gain connectivity.

Case Study

AgriDigital

Based in Sydney, AgriDigital provides software solutions to simplify commodity management, improve supply chain finance and bring traceability to agribusinesses. Using cloud based applications and blockchain technology, the company provides transactional and payment security for participants along agri-supply chains, thus proving product integrity and improving today's disconnected and siloed supply chains.

A recent blockchain pilot run by AgriDigital in conjunction with CBH Group at their oat processing facility aimed to test ways blockchain may deliver increased efficiencies and reduce supply chains risks in the grains industry. Using a private blockchain, AgriDigital and CBH traced the movement of a batch of organic oats from the farmgate, through milling and production, to a retail consumer. Data on the provenance, movement and treatment of the oats from the farmgate, through milling and production, to a retail customer was stored and analysed on a private network. As a blockchain is an immutable record of data, it is critical to ensure both the data and the user are correctly identified prior to sharing of data.[97]

With digital uptake being very low across Australia's agriculture sector,[98] the development of novel cyber security products and services could work to ease the concerns of the agriculture industry, including around data ownership and sharing, thereby enabling businesses to feel comfortable to participate in the data world.

97 AgriDigital (2017). *Pilot Report: Solving for supply chain inefficiencies and risks with blockchain in agriculture.*
98 McKinsey & Company (2017). *Digital Australia: Seizing the opportunity from the Fourth Industrial Revolution.*

Priority Action 2: Improve collaborative data sharing

Theme: Trusted ecosystem

Adoption of digital technologies in the food and agribusiness industry will not only help improve productivity, but is a key contributor to the development of premium foods, especially for improved traceability technologies. However, adoption of these digital technologies can be challenging, especially for agribusinesses – an industry that has a lower level of digital maturity than many other industries.[99] The recently established Food Agility CRC aims to help Australia's food and agribusiness industry to grow its comparative advantage through digital transformation, with research programs aimed at promoting data sharing.[100]

Within the food and agribusiness industry, more activities are needed to build business confidence in the privacy, security and ownership of data throughout the supply chain. To generate added value from an individual organisation's data, it generally needs to be aggregated with data from different sources in order to produce actionable insights. To facilitate trusted data sharing activities, an ecosystem of trust needs to be established, with appropriate protections in place for ownership and privacy of data, alongside division of added value coming from data.

To improve collaborative data sharing, the food, agribusiness and cyber security ecosystem should:

- Participate in the development of appropriate frameworks to help establish best practice for food and agribusiness data sharing within the supply chain or broader ecosystem. These frameworks will help build trust and confidence required to engage in data sharing with service and technology providers.
- Work with the food and agribusiness supply chain to assemble a consortium of participants to trial and demonstrate ways that data can be shared among participants in a trusted fashion, to the benefit of all. This will help to build the business case for integration of digital technologies, including (but not limited to) advanced traceability systems. Cyber security innovation will be key to establishing trust in this demonstration project, and beyond.
- Develop tools to enable participants in the food and agribusiness industry to store, access, re-use and market their own data with appropriate protections of ownership and privacy in place.

The Food Agility CRC[101]

The Food Agility CRC aims to empower Australia's food industry to grow its comparative advantage through digital transformation. While Australia has a comparative advantage in agriculture with a reputation for quality and safety, changing consumer preferences and increasing competition mean that a more concentrated effort will be required to nurture and maintain this comparative advantage into the future. The Food Agility CRC brings together participants from the food, technology and research sectors to develop and use digital technologies for sharing data to build brand, markets, jobs and exports across the Australian food value chain.

99 McKinsey & Company (2017). *Digital Australia: Seizing the opportunity from the Fourth Industrial Revolution.*
100 Food Agility CRC (n.d.). [Online] Available from: http://www.foodagility.com/ Accessed: 12/03/2018
101 Food Agility CRC (n.d.). [Online] Available from: http://www.foodagility.com/ Accessed: 12/03/2018

Future research priorities

Research priorities underpinning the growth of this sector include:

- development of technologies that can provide food safety assurance and negate the impact of food fraud[102]
- innovation in endpoint authentication and identity management, including people and business identity to enable identity-centred supply chain integrity
- innovation in the secure management of digital food and agribusiness production and processing operations, including connected machinery and methods for data transfer
- improved platforms and systems for finance and insurance – for example, enabling the use of smart contracts to facilitate secure payments or blockchain for traceability from farm to shelf
- secure methods for integration of additional, trusted data from various sources throughout the supply chain
- advanced and secure electronic sensors and biosensors for condition monitoring, and smart and intelligent food packaging.

Food fraud costs the global food industry an estimated AU$50 billion each year.[103]

Case Study

The Entrepreneurs' Programme

The Entrepreneurs' Programme is the Australian Government's flagship initiative for business competitiveness and productivity. The Programme provides Australian businesses with quality advice and support to innovate and grow. Throughout 2017, the Entrepreneurs' Programme, in collaboration with Hivint Pty Ltd, delivered a series of cyber security webinars for Australian SMEs to educate and raise awareness of cyber security solutions and practices. The webinar series was advertised widely to SMEs across the country, including food and agribusinesses, and covered topics such as:

- cyber security for small to medium enterprises
- the cyber threat landscape for small to medium enterprises
- cyber security operational basics
- developing an effective incident response capability
- cyber security in the cloud and outsourcing.

The webinar series were well attended and armed participant's with simple steps to plan, adapt and respond to the changing cyber landscape.

102 Food Innovation Australia Ltd (2017). *Sector Competitiveness Plan – Food and Agribusiness Growth Centre.*
103 McLeod, R. (2017). *Counting the Cost: Lost Australian food and wine export sales due to fraud.* Food Innovation Australia Ltd.

Catalysing growth

5 Catalysing growth

Working together with Australian businesses, cyber security companies will enable economic growth through trusted integration of digital technologies, thus allowing organisations to become more innovative. This initiative is also intended to mitigate cyber threats.

In addition to empowering Australian industry, cyber security presents an opportunity for Australia to develop a new, high-growth, globally-competitive export industry that will provide solutions and services to companies and governments around the world.

This Roadmap details three change themes which in combination will propel the growth of Australia's cyber security sector. Across Australia's priority growth sectors and beyond, the suggested industry actions under these themes will help to improve data sharing and trust in the digital ecosystem, increase proactive consideration of cyber security in new products and services, and foster a robust cyber security culture. Recognising that people are often the most vulnerable element in cyber security defences, improvements in education, training and awareness are important.

FIGURE 12: CYBER SECURITY GROWTH THEMES AND PRIORITY ACTIONS

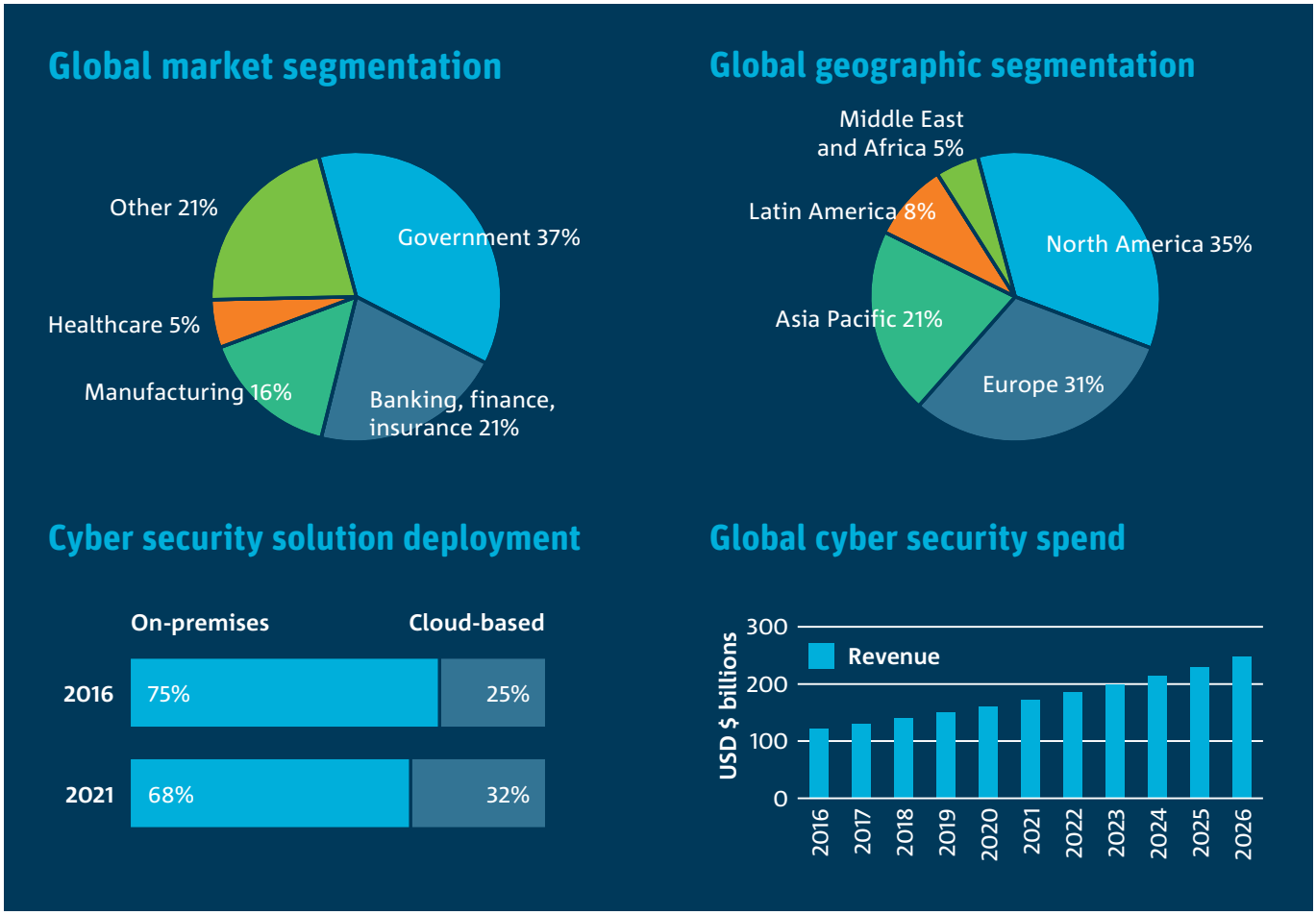
Appendix

6 Appendix

A.1 The global cyber security market

Globally, the market for cyber security products and services is growing and is projected to increase by 88% by 2026. In 2017, the global cyber security budget was estimated to be worth around US$131 billion, with 75% made up by organisations' and individuals' purchasing solutions from external cyber security businesses, with the remaining spent on in-house capabilities.

FIGURE 13: GLOBAL CYBER SECURITY MARKET SNAPSHOT, 2016[104 105]



104 Technavio (2017). *Global cyber security market 2017-2021.*
105 Australian Cyber Security Growth Network Ltd (2018). *Cyber Security Sector Competitiveness Plan.*

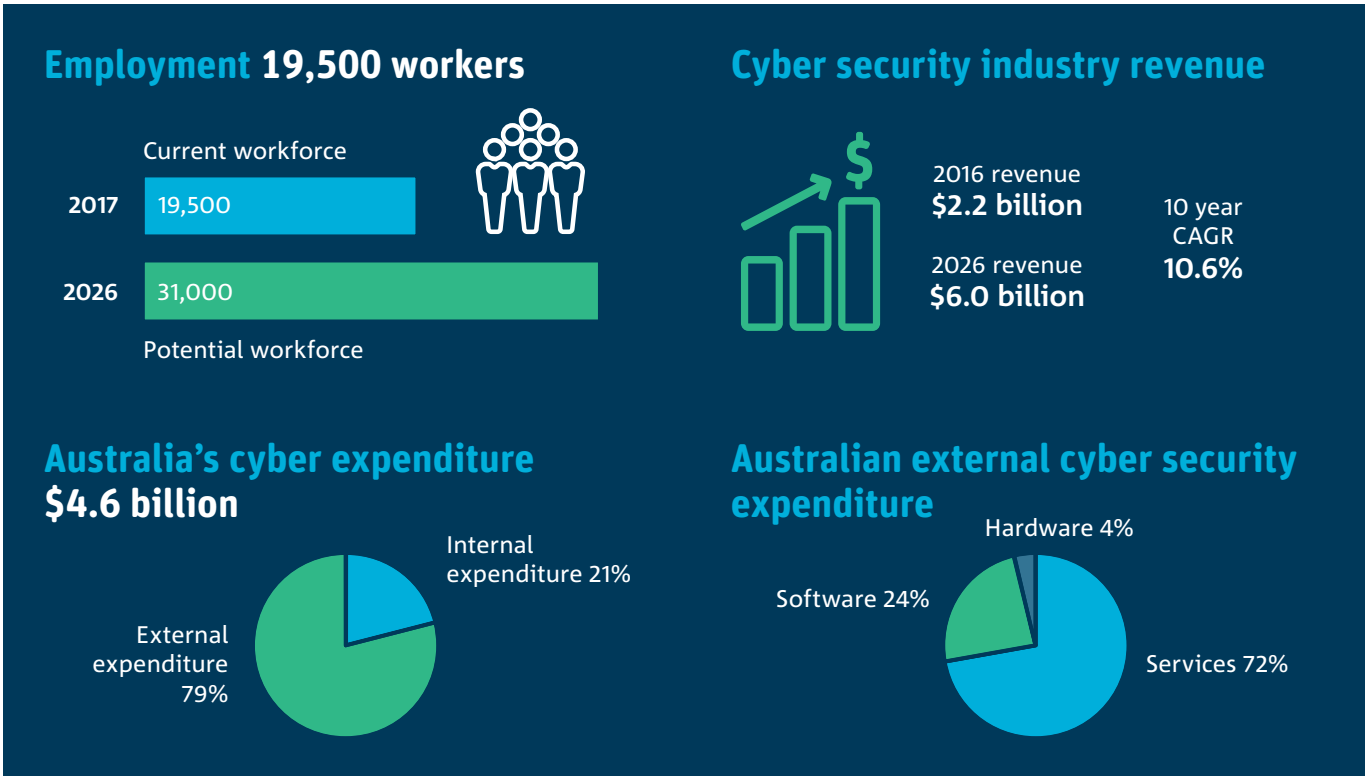
A.2 The Australian cyber security market

Supporting and developing a vibrant Australian cyber security sector, with a critical mass of experts is important for the growth and prosperity of the Australian economy, as well as for national security.[106] Digitisation and digitalisation have provided numerous benefits to governments, industry and the individual. However, they have also allowed for an increase in unauthorised access to data and cyber-physical systems, which can erode trust in digital technologies. In 2015, the average cost of a cyber-attack on an Australian business was AU$419,000 and took 31 days to resolve.[107] The business disruption and cost associated with cybercrime, together with customer expectations, will drive growth in both the global and Australian cyber security sectors.

Currently, the cyber security sector is small but fast-growing. In the future, it faces great economic opportunity arising from the burgeoning global market for cyber security solutions and an expected surge in domestic demand.

The Australian cyber security sector consists of external and internal providers. External cyber security providers deliver services, hardware and software to users (i.e. organisations and individuals looking to defend themselves against malicious cyber activity), while internal cyber security refers to users with their own in-house specialised cyber security functions. Within the Australian business community, the majority of organisations lack the capacity to employ large internal cyber security teams, creating demand for external cyber services. The 2018 update to AustCyber's Cyber Security Sector Competitiveness Plan provides a deeper analysis of the projected size and shape of the cyber security market, together with a high-level categorisation of the sector.

FIGURE 14: AUSTRALIAN CYBER SECURITY MARKET SNAPSHOT, 2017[108]

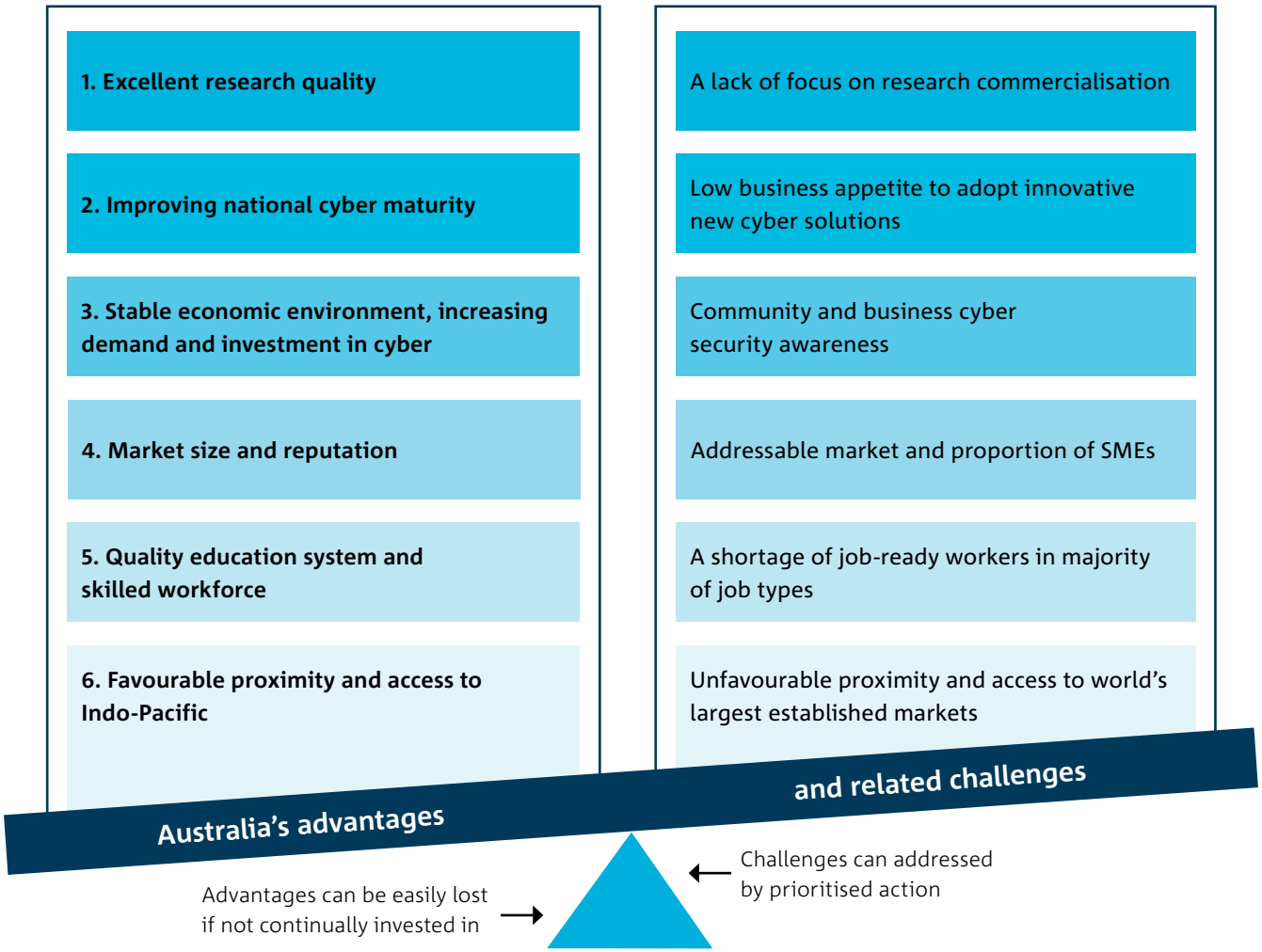


106 Department of the Prime Minister and Cabinet (2016). *Australia's Cyber Security Strategy, p. 4.* Commonwealth of Australia.
107 Ponemon Institute (2015). *2015 Cost of Cyber Crime Study: Australia,* Michigan.
108 Australian Cyber Security Growth Network Ltd (2018). *Australia's Cyber Security Sector Competitiveness Plan - 2018 Update.*

A.3 Australia's advantages and related challenges

Australia's cyber security sector is underpinned by a number of unique advantages and related challenges. Businesses should seek to build on these advantages and address challenges as they grow.

FIGURE 15: AUSTRALIA'S ADVANTAGES AND RELATED CHALLENGES



1. Excellent research quality

Australia has world-class cyber security research, with strengths in core research areas including quantum computation, wireless technology, trustworthy systems and niche high-value hardware.[109] Australia's strength in cyber security research is exemplified by its many dedicated research institutions and centres, including CSIRO's Data61, the Defence Science and Technology Group (DSTG), the Cyber Security Research Centre, the Oceania Cyber Security Centre, and a number of Cooperative Research Centres (CRCs), including the Data to Decisions CRC and the Cyber Security CRC. Many universities across Australia also have dedicated research centres. Australian cyber security research papers are ranked first in terms of their citation impact, attaining the highest number of citations globally.[110] Australia's strengths are further cemented by pockets of commercial R&D on complex, deep technical challenges.

Related challenge: A lack of focus on research commercialisation

Competitiveness in cyber security is highly dependent on R&D. Despite the quality and quantity of Australian cyber security research, a lack of national coordination on delivering outcomes against strategic level research themes (provided by the Commonwealth Research Priorities, DSTG, Data61 and the knowledge priorities in the Cyber Security SCP) and poor collaboration undermine the commercialisation of Australian research into marketable products and services. Inadequate incentives for commercialisation also weaken Australia's ability to lead on innovation in cyber security.[111] Furthermore, the penetration of multinational cyber security corporations in Australia results in a high level of imports, paired with offshore R&D.

2. Improving national cyber maturity

Australia was ranked seventh most committed nation in the International Telecommunication Union's 2017 Global Cybersecurity Index,[112] which takes into account five key pillars: legal, technical, organisational, capability building and cooperation. Within the Asia-Pacific region, the Australian Strategic Policy Institute (ASPI) has ranked Australia highly for its cyber maturity, based on the country's investment in governance and implementation of the 2016 Cyber Security Strategy.[113] While there is more to do with regards to the cyber maturity in the business community and Australian society more broadly, there are promising signs this is improving.

Related challenge: Low business appetite to adopt innovative cyber solutions

Cyber security start-ups often struggle to engage their first customer. Industry consultation outlined that there is low trust and general risk aversion in the business community towards adoption of home-grown Australian innovations, which is a significant hurdle for new businesses. Strict procurement rules in many government agencies (at all levels) and private-sector companies favouring larger, established businesses (often multinationals) means that engagement with cyber security providers only occurs with those that have a proven track record.[114] Many Australian cyber security businesses also tend to undervalue and undersell aspects of their offerings that are critical for local customers. Other aspects of Australian culture also present challenges to growth, including discomfort with 'tall poppies', fear of failure and not celebrating successes.

109 Australian Trade and Investment Commission (2017). *Cyber Security*, Commonwealth of Australia.

110 Australian Government (2015). *Science and Research Priorities Cyber Security – Capability Statement* [Online] Available from: http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Documents/Science-Research-Priorities-Cybersecurity.pdf Accessed: 27/02/2018

111 Australian Cyber Security Growth Network Ltd (2018). *Australia's Cyber Security Sector Competitiveness Plan - 2018 Update.*

112 International Telecommunication Union (2017). *Global Cybersecurity Index (GCI) 2017*, [Online] Available from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf Accessed: 27/02/2018

113 Australian Strategic Policy Institute (2017). Cyber maturity in the Asia-Pacific Region 2017, Barton.

114 Australian Cyber Security Growth Network Ltd (2018). *Australia's Cyber Security Sector Competitiveness Plan - 2018 Update.*

3. Stable economic environment, increasing demand and investment in cyber

Australia's sound governance, economic stability, low sovereign risk and high living standards act as drawcards for foreign investment.[115] Government policy – both in terms of support for cyber security and open data – is favourable, with the Global Open Data Index ranking Australia the second nation in the world for its open government data policies.[116] Data61 is working with the Australian Government to increase availability and insights gained from high-value government datasets.[117] One example is the National Map – a map based visualisation and access tool for open government data stored on data.gov.au, with software developed by Data61.[118] The Data Integration Partnership for Australia (DIPA) aims to create new insights to answer complex policy questions by using integrated data.[119]

Australia's Cyber Security Strategy has catalysed rapid growth in interest, energy and focus across the cyber security sector, with cyber security being recognised as an area of Australian competitive strength and strategic priority. This has led to the establishment of AustCyber, as well as an AU$50 million investment in a cyber security CRC, the appointment of a Special Adviser to the Prime Minister on Cyber Security (now known as the National Cyber Security Adviser), alongside the appointment of an Australian Cyber Ambassador, resulting in the development of Australia's International Cyber Engagement Strategy. Furthermore, the development of the Joint Cyber Security Centre (JCSC) program and numerous research centres illustrates the growing focus on cyber security.

Related challenge: Community and business cyber security awareness

Despite the fact that it is a priority growth sector for the Australian Government, community and business awareness of the importance of cyber security is still comparatively low. While high-profile incidents increase awareness, ideally cyber security should be proactive, not simply reactive to cyber incidents (also resilience poses lower operational costs). Alongside low awareness of cyber security, SMEs have limited budgets and resources, and generally lack technical knowledge and processes to react to cyber threats. Compared to most other nations, Australia's higher than average income and limited awareness of cyber security results in the community and small businesses being highly vulnerable to cybercrime.

---

4. Market size and reputation

Australia's economy shares many similarities with its larger peers but at a smaller scale. Australians also have a reputation as 'early adopters' of technology. This makes Australia an ideal place for a range of local and international businesses to test cyber-oriented products and services, as they are able to implement a full system at a smaller scale and gather critical feedback prior to a global launch.[120] Digitisation of Australia's industries is creating strong demand for cyber security, particularly for services, meaning there are commercial opportunities for cyber security businesses in Australia. Industry development also benefits from 'Brand Australia' and Australia's reputation for innovation, creativity, technology and science.

Related challenge: Addressable market and proportion of SMEs

Australia's small market size also presents a number of challenges, with the addressable market in Australia being smaller than in other countries. By volume, small to medium enterprises (SMEs) account for the majority (99.8%) of registered businesses in Australia and account for approximately half of Australia's GDP.[121] The needs of SMEs in terms of cyber security are diverse and present a challenging local environment for new cyber security businesses to reach critical mass. For this reason, Australia's global reputation is fragile and needs to be protected.

115 Australian Trade and Investment Commission (2018). *Why Australia Benchmark Report 2018,* Commonwealth of Australia.

116 Open knowledge international (2017). *Global Open Data Index – Australia*, [Online] Available from: https://index.okfn.org/place/au/ Accessed: 27/02/2018

117 Data61 (n.d.). *Platforms for Open Data,* [Online] Available from: https://data61.csiro.au/en/Collaborate-with-us/Government/PFOD-Projects Accessed: 16/03/2017

118 Department of the Prime Minister and Cabinet, Department of Communications, and CSIRO Data61 (2017) *About National Map,* [Online] Available from: https://nationalmap.gov.au/about.html Accessed: 27/02/2018

119 Department of the Prime Minister and Cabinet (n.d.), *Data Integration partnership for Australia,* [Online] Available from: https://www.pmc.gov.au/public-data/data-integration-partnership-australia Accessed: 16/03/2018

120 Australian Government (2015). *Science and Research Priorities Cyber Security – Capability Statement* [Online] Available from: http://science.gov.au/scienceGov/ScienceAndResearchPriorities/Documents/Science-Research-Priorities-Cybersecurity.pdf Accessed: 27/02/2018

121 The Australian Small Business and Family Enterprise Ombudsman (2016). *Small Business Counts—Small Business in the Australian Economy*, Commonwealth of Australia.

5. Quality education system and skilled workforce

Globally, Australia is ranked ninth for higher education and training by the World Economic Forum.[122] Tertiary level education rates in Australia are well above the OECD average[123] and have grown at a steady rate for two decades. High education levels are important as the growth of Australia's cyber security industry will require a greater number of highly-skilled professionals relative to other sectors (refer to the 2018 SCP update).

Related challenge: A shortage of job-ready workers in majority of job types

Australian cyber security businesses are struggling to attract the right skills for their businesses, which is caused by the inability of education providers to rapidly produce more cyber security graduates and the failure of many workplaces to offer on-the-job training.[124] Furthermore, Australia is at risk of losing key talent in the cyber security industry, with overseas recruiters increasingly successful in luring Australia's top talent.[125] Skills shortages not only affect Australia's cyber security sector, but could leave Australian industry overall more vulnerable to cyber-attack. Rectifying the national skills shortage is a key goal of AustCyber, in partnership with other key stakeholders.

---

6. Favourable proximity and access to Indo-Pacific

Australia is well placed to serve Indo-Pacific markets (encompassing Northeast and Southeast Asia, Pacific, the US and Indian Ocean states) both in terms of geographic proximity and shared time zones across major population centres. Being within the same time zones as major Asian countries and industry players enhances Australia's ability to develop working relationships with stakeholders in the world's fastest growing economic region. Approximately 21% of Australians speak a language other than English, with the most common being Mandarin, Cantonese and Vietnamese.[126] These strong ties to growing economies in the Indo-Pacific region are an inherent advantage for Australian cyber security.

Related challenge: Unfavourable proximity and access to world's largest established markets

While Australia's location is favourable for Indo-Pacific markets, the tyranny of distance and different time zones is unfavourable for interactions with key markets in Europe and USA, and generally results in higher trading costs.

122 Schwab, K. et al (2016). *The Global Competitiveness Report 2016–2017*, World Economic Forum, Geneva.
123 OECD (2015). *Australian manufacturing in the global economy, p. 58*.
124 Australian Cyber Security Growth Network Ltd (2017). *Cyber Security Sector Competitiveness Plan, p. 61*.
125 Australian Cyber Security Growth Network Ltd (2017). *Cyber Security Sector Competitiveness Plan, p. 71*.
126 Australian Bureau of Statistics (2017). *Census reveals a fast-changing, culturally diverse nation*, [Online] Available from: http://www.abs.gov.au/ausstats/abs@.nsf/lookup/Media%20Release3 Accessed: 27/02/2018

A.4 Further Reading

Cyber Security

Australian Cyber Security Growth Network (2018). *Cyber Security Sector Competitiveness Plan – 2018 update*.

Commonwealth of Australia, Department of the Prime Minister and Cabinet (2016). *Australia's Cyber Security Strategy*.

Commonwealth of Australia, Department of Foreign Affairs and Trade (2017). *Australia's International Cyber Engagement Strategy*.

Commonwealth of Australia, Australian Cyber Security Centre (2017). *Australian Cyber Security Centre 2017 Threat Report*.

Australian Strategic Policy Institute (2017). *Cyber Maturity in the Asia–Pacific Region 2017*.

ASX (2017). *ASX 100 Cyber Health Check Report*.

Medical Technologies and Pharmaceuticals

CSIRO (2017). *Medical Technologies and Pharmaceuticals – A Roadmap for unlocking future growth opportunities for Australia*.

MTPConnect (2016). *Medtech, Biotechnology and Pharmaceutical Sector Competitiveness Plan*.

Australian Council of Learned Academies (2018). *The Future of Precision Medicine in Australia*.

Commonwealth of Australia, Australian Digital Health Agency (2017). *Australia's National Digital Health Strategy*.

Mining Equipment, Technology and Services

CSIRO (2017). *Mining Equipment, Technology and Services – A Roadmap for unlocking future growth opportunities for Australia*.

METS Ignited (2016). *Mining Equipment, Technology and Services 10 Year Sector Competitiveness Plan*.

WillisTowersWatson (2017). *From technology to people: The new frontier in mining cyber risk*.

Deloitte (2017). *Tracking the trends 2017 – The top 10 trends mining companies will face in the coming year*.

Advanced Manufacturing

CSIRO (2016). *Advanced Manufacturing – A Roadmap for unlocking future growth opportunities for Australia*.

Advanced Manufacturing Growth Centre (2017). *Sector Competitiveness Plan 2017*.

Swinburne University of Technology, Prime Minister's Industry 4.0 Taskforce (2017). *Industry 4.0 Testlabs in Australia – Preparing for the Future*.

Deloitte (2016). *Cyber risk in advanced manufacturing*

Oil and Gas

CSIRO (2017). *Oil and Gas – A Roadmap for unlocking future growth opportunities for Australia*.

National Energy Resources Australia (2017). *Sector Competitiveness Plan 2017*.

DNV GL (2015). *Industry perspective: Digitalization in the oil and gas sector*.

EY (2017). *Digitization and cyber disruption in oil and gas*.

Food and Agribusiness

CSIRO (2017). *Food and Agribusiness – A Roadmap for unlocking value-adding growth opportunities for Australia*.

FIAL (2017). *Sector Competitiveness Plan – Food and Agribusiness Growth Centre*.

McLeod, R., (2017). *Counting the Cost: Lost Australian food and wine export sales due to fraud,* Food Innovation Australia Ltd.

Leonard, E., et al (2017). *Accelerating precision agriculture to decision agriculture: Enabling digital agriculture in Australia,* Cotton Research and Development Corporation, Australia.

CONTACT US
t 1300 363 400
+61 3 9545 2176
e csiroenquiries@csiro.au
w www.csiro.au

WE DO THE EXTRAORDINARY EVERY DAY

We innovate for tomorrow and help improve today – for our customers, all Australians and the world.

Our innovations contribute billions of dollars to the Australian economy every year. As the largest patent holder in the nation, our vast wealth of intellectual property has led to more than 150 spin-off companies.

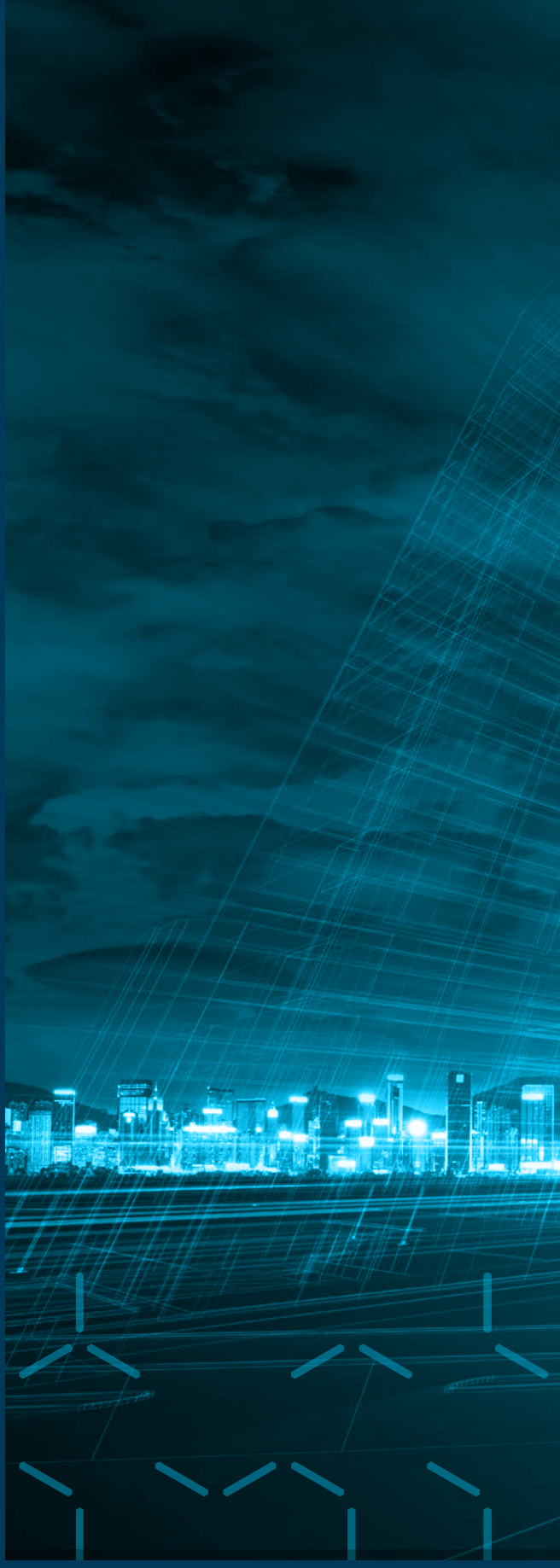
With more than 5,000 experts and a burning desire to get things done, we are Australia's catalyst for innovation.

WE IMAGINE
WE COLLABORATE
WE INNOVATE

FOR FURTHER INFORMATION
Dr Liming Zhu
Research Director, CSIRO's Data61
t +61 2 9490 5638
w www.data61.csiro.au

James Deverell
Director, CSIRO Futures
t +61 2 9490 8456
e futures@csiro.au
w www.csiro.au/CSIROfutures

Michelle Price
Chief Executive Officer, AustCyber
t +61 2 9239 3250
e info@acsgn.com
w www.AustCyber.com



B&M | 18-0097