Industry Report

Cyber Security – Australia

Prepared by:

Foley & Associates
Suite 48/L9, 88 Pitt Street
Sydney, NSW, 2000
Tel: +61 2 9229 8556
Email: holden@foley.net.au

Date: 12 June 2019

VEDP | Virginia Economic Development Partnership

Contents

EXECUTIVE SUMMARY

As the Australian Global Network Consultant to the Virginia Economic Development Partnership (VEDP), Foley & Associates was commissioned to prepare an in-depth industry report on the **Cyber Security sector in Australia**.

This report is intended to provide Virginian exporters with a general overview of Australia's cyber security sector, as well as offer specific insights into the status of cyber security in Australia's health care, defense, critical infrastructure and banking, financial services & insurance (BFSI) sectors.

We have structured this report into the following sections:

- **Overview & Current Status of the Australian Cyber Security Sector** (which includes Recent Developments & Industry Opportunities)**;**
- **Key Players;**
- **Local Legislation & Regulators;** and
- **Market Entry Options.**

This report also provides information regarding:

- **Industry Publications;**
- **Industry Events;** and
- **Recent examples of Cyber Attacks / Data Breaches.**

We encourage any Virginian companies with questions or enquiries to contact VEDP for further information.

We look forward to continuing to assist VEDP and Virginian exporters in the Australian market.

Sydney, 12 June 2019

INTRODUCTION

ECONOMIC OVERVIEW

As one of the richest nations in the world, Australia is currently in a strong economic position. Over the last quarter century, Australia's **medium-sized AU$1.7 trillion economy (~US$1.2 trillion)** (**ranked 14th in the world)**, has proven exceptionally resilient, recording **27 years of uninterrupted economic growth**. This growth was catalysed in part by microeconomic reform and a productivity boost in the 1990s, and then fuelled by a terms-of-trade boom after 2000, as a global rise in resource prices increased the value of Australia's commodity exports.

Since their peak in 2011, however, Australia's terms of trade have fallen by over 30%. According to the Australian Treasury, in order to achieve a long-run trend rate of 2% growth in GDP – which is required to maintain current standards of living – **Australia requires an annual productivity growth of 2.5% a year**. Based on current figures, **this cannot be achieved by increases in labour productivity alone**, which over the five years to 2015-16 remained at 1.8%. Australia therefore needs to find new ways to lift its productivity and identify new sources of export competitiveness to ensure its future economic prosperity.

WHY AUSTRALIA?

Australia is a suitable **investment location** and **trading partner** for Virginian exporters due to the ease of doing business and the existence of:

- ✓ A large services economy;
- ✓ A quality education system;
- ✓ Sound governance settings;
- ✓ Economic stability;
- ✓ Low sovereign risk; and
- ✓ High living standards.

In regards to Cyber, maturity in Australia's cyber security sector means that Australia is well positioned to provide an **ideal growth environment for cyber businesses**, with existing strengths in core research areas such as quantum computation, wireless technology, trustworthy systems and niche high-value hardware.

Whilst the global cyber security market is forecast to grow rapidly over the coming years, cyber security spending in the Indo-Pacific region is expected to increase faster than the global average. Several Indo-Pacific countries (e.g. China, India, Malaysia, Singapore) are emerging as significant buyers of cyber security solutions, and according to AustCyber's Cyber Competitiveness Plan (2018), the region will account for approximately one-quarter of global cyber security spending by 2026.

Australia's **geographic proximity to these fast-growing and increasingly digitized countries** will be beneficial to Virginian companies looking to explore potential opportunities in both Australia and the wider region.

Please refer to the Appendix for further information on opportunities vs. challenges in the Australian cyber security environment.

KEY FINDINGS

- ✓ Industry revenue of the Australian cyber security sector was A$2.2 billion (~US$1.5 billion) in 2016, however it is **forecast to almost triple to reach ~A$6 billion (~US$4.2 billion) by 2026** (CSIRO / AustCyber).

- ✓ Growth in the sector is being driven by the **volume of increasingly sophisticated cyber-attacks**, **mounting exposure** to cyber risk due to the rapid uptake of interconnected and digital devices, and **increased awareness**, which is leading to the implementation of new strategies, frameworks, regulations and standards.

- ✓ Cyber security is an **issue of national importance** resulting in **proactive strategies to drive industry growth and expertise**. The national Cyber Security Strategy, AustCyber's Australia's Cyber Security Sector Competitiveness Plan, and the CSIRO/AustCyber Cyber Security Roadmap are examples of recent strategies.

- ✓ The Government is **increasing funding** throughout the industry. In May 2019, the federal government committed to providing A$156 million in funding (~US$109 million) to boost the Australian cyber security sector.

- ✓ Cyber security is an important consideration for companies and a key enabler of growth in a range of industry sectors. **Critical Infrastructure** (i.e. the essential services and systems in the banking, financial services, defense, communications, energy, resources, health, transport and water sectors) are the main targets of cyber-attacks, and therefore represent the **sectors with the greatest opportunity for Virginian exporters.**

- ✓ **79% of all cyber security spending in Australia is delivered through external parties** demonstrating limited in-house cyber security capability in Australia.

- ✓ International companies currently supply approximately 50% of all cyber security products and services in Australia. **Australia imported ~A$1.6 billion (~US$1.1 billion) of cyber security products and services in 2017.**

- ✓ Virginian companies interested in exploring opportunities in the Australian market are encouraged to first review **local legislation**, engage with **key industry associations**, and subscribe to relevant **industry publications** to remain abreast of current issues and developments in the sector.

- ✓ The VEDP Trade Mission to Australia in October 2019 aligns with one of the key industry sector events – the Australian Cyber Conference 2019.

- ✓ This report will further assist Virginian companies to develop a suitable **market entry strategy** for the Australian market to align with their overall objectives.

CURRENT TRENDS SUMMARY

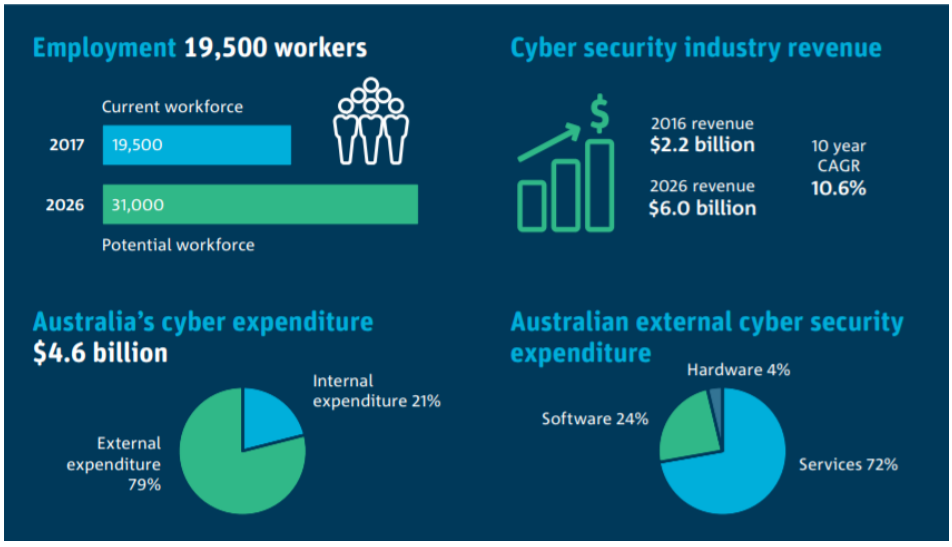
AUSTRALIA'S CYBER SECURITY SECTOR

The Australian Government has identified cyber security as an industry sector that is vital to Australia's long-term economic prosperity and national security. The development of a thriving and globally competitive cyber security sector in Australia will improve overall national security, promote greater trust in Australia as a safe and desirable country for potential international investors and trading partners, and contribute to the domestic and international success of other Australian industries such as medtech & pharmaceuticals, mining, advanced manufacturing, food & agribusiness etc.

Australia spends approximately **A$4.6 billion** (~US$3.2 billion) on cyber security products and services each year.

Currently, the majority of Australian organizations lack the capacity to employ large internal cyber security teams, creating demand for **external**, often **international cyber services**. According to AustCyber, approx. 79% of Australia's cyber expenditure is external, whilst only 21% is internal expenditure.

However, due to increasing demand for cyber security products and services, Australia's cyber security sector is forecast to grow rapidly over the next seven years to reach **industry revenue of A$6 billion (~US$4.2 billion) and employ 31,600 people by 2026**.



Source: CSIRO Futures / AustCyber

The growth of the Australian cyber security sector is being driven by:

- ✓ The growing **volume of malicious cyber activitity** and the use of increasingly **sophisticated strategies** to infiltrate systems and networks;
- ✓ Mounting **exposure to cyber risk** due to the rapid expansion of internet-enabled economic activity, the increasing volume and quality of information shared elecontronically, and the widespread adoption of connected devices and systems that are susceptible to malicious cyber activity;

- ✓ **Growing awarness** of the potential risks, physical and economic impacts of cyber attacks as a result of recent high-profile cases and media coverage, which is driving companies to implement **cyber preparation strategies and frameworks**, including security audits, risk assessments, compliance tools and end-user training; and

- ✓ The **increasing regulation** of cyber risk through the development of new laws (e.g. the Notifiable Data Breach scheme) and mandatory standards, which is leading businesses to increase their spending on cyber security products and services.

  Several recent examples of cyber attacks / data breaches have been provided as an Appendix to this report for reference.

CURRENT STATUS OF CYBER SECURITY IN AUSTRALIA

Whilst Australia's cyber security sector is still developing, it has the potential to capture a significant share of the global cyber security market, which is forecast to grow by 88% over the next eight years to reach a value of approximately **US$250 billion by 2026**.

According to AustCyber (www.austcyber.com), Australia's commitment to cyber security and current level of cyber maturity makes Australia an ideal growth environment for cyber businesses:

- ✓ The International Telecommunications Union's 2018 Global Cybersecurity Index ranked Australia as the **third most committed country to cyber security in the Indo-Pacific region** (after Singapore and Malaysia), and the **tenth most committed country globally.**

- ✓ Results from the Cyber Maturity in the Asia-Pacific Region survey* conducted by the Australian Strategic Policy Institute in 2017 indicated that **Australia's level of cyber maturity is second highest in the Indo-Pacific region** (equal to Japan), after the US which was ranked first.

  *Note: the survey assesses the **cyber maturity** of countries, based on how well governments worldwide invest in cyber security policies and legislative structures, business and digital economic strength, responses to financial cybercrime, military organization, and social cyber awareness.

- ✓ Australia was ranked **second globally** in the 2017 Global Open Data Index, which measures policies that support cyber security and allow government data to be openly available to the public.

RECENT DEVELOPMENTS

Australia's Cyber Security Strategy

The first national Cyber Security Strategy was released by the Australian Government in 2016. This Strategy elevated cyber security to an **issue of national importance** and led to the establishment of AustCyber, the Australian Cyber Security Growth Network.

The Strategy, backed by approximately A$230 million (~US$161 million) of government funding, outlined the following **five key themes** and corresponding initiatives that the Australian Government intends to achieve by 2020.

1. A National Cyber Partnership

The Australian Government intends to foster effective collaboration between the public sector, industry and the research community, in order to set the strategic agenda, tackle emerging cyber security issues, and better understand the costs of malicious cyber activity.

The Government is also aiming to streamline cyber security governance, establishing clear responsibilities across government agencies.

2. Strong Cyber Defenses

Australian government agencies and businesses need to improve their cyber security performance and to detect, deter and respond to cyber security threats more effectively. To do so, the government has committed to investing in the Australian Cyber Security Centre as well as the development of an online cyber threat sharing portal.

3. Global Responsibility and Influence

The Australian Government has committed to collaborating with international law enforcement and intelligence agencies to address cyber security threats, build cyber capacity, and prevent safe havens for cyber criminals.

4. Growth and Innovation

To take advantage of the growing global market for cyber services, the Government is supporting the expansion, diversification and development of companies within Australia's cyber security sector by encouraging R&D initiatives and promoting innovation in Australia through the establishment of the Cyber Security Growth Centre.

5. A Cyber Smart Nation

Addressing the critical shortage of skilled cyber security professionals underpins the overall success of Australia's Cyber Security Strategy. The government has worked with academic and research institutions to establish academic centers of cyber security excellence that are linked to other initiatives in Australia (e.g. the Cyber Security Growth Centre) as well as other internationally recognized universities.

The Government also intends to improve national cyber security awareness through joint public-private initiatives and education campaigns, ensuring all Australians understand the potential risks and how to protect themselves online.

Australia's Cyber Security Sector Competitiveness Plan

In 2018, AustCyber released an update to Australia's Cyber Security Sector Competitiveness Plan, reflecting the rapid evolution of the sector since April 2017 when the first iteration of the Plan was released.

According to AustCyber, Australia must address the following major challenges in order to develop a world-class cyber security sector:

- ✓ Address the current **skills shortage** and **workforce gap**;
- ✓ Focus on **research & development**;
- ✓ Improve the **incubation environment** for startups; and
- ✓ Enhance access to **global markets**.

To remain globally competitive, Australian industry must also work towards a state where all businesses demonstrate sophisticated, robust and resilient cyber security culture. This will require industry to shift its perceptions of cyber security from a risk and compliance-based requirement to an **essential business function** underpinning economic growth.

AustCyber's research indicates that **approximately 62% of Australian companies are looking to increase their overall security spending** over the next 1-2 years.

In particular, demand for **cyber services** is predicted to experience significantly higher growth in comparison to software and hardware over the next decade, as Australian SMEs increasingly outsource services to manage growing security needs and more sophisticated security breaches.

Australian Cyber Security Industry Roadmap

The Commonwealth Scientific and Industrial Research Organization (CSIRO), in collaboration with AustCyber, released the Cyber Security Roadmap in 2018.

The Roadmap highlights the potential of cyber security solutions to enable growth for a wide range of industry sectors:

Source: CSIRO Futures/AustCyber

Based on industry consultation conducted by CSIRO and AustCyber, **three key themes** required to improve Australia's overall security posture and take advantage of digital transformation are:

1. **Trusted Ecosystem:** Creating highly trustworthy digital ecosystems that allow for the rapid exchange of information and provide a **stronger environment for trade**.

2. **Secure by Design:** Ensuring new products, services, platforms and processes are designed with **cyber security as a key consideration**.

3. **Robust and Resilient:** Developing a robust security culture to build greater **cyber maturity and resilience** in Australian industry and communities.

Government Funding & Planned Initiatives

In the lead-up to the Australian federal government election in May 2019, the Australian Liberal Party (who were successfully re-elected) committed to providing A$156 million in funding (~US$109 million) to boost the Australian cyber security sector through several key initiatives, including:

- ✓ The creation of an A$50 million (~US$35 million) **Cyber Security National Workforce Growth Program**;

- ✓ The establishment of a new A$40 million (~US$28 million) **Countering Foreign Cyber Criminals** capability;
- ✓ A further A$26 million (~US$35 million) to support the **Australian Cyber Security Centre**;
- ✓ The creation of **cyber security 'SPRINT' teams**;
- ✓ The development of a **Cyber Security Response Fund**; and
- ✓ A$40 million (~US$28 million) funding to assist the **Australian Defense Force** to grow its **cyber warfare workforce**, creating 230 new military cyber specialist positions through to 2022-23.

The second round of the AustCyber Projects fund, a A$15 million (~US$10.5 million), three-year initiative designed to assist Australia's cyber security capability grow and expand internationally, is currently open until 12 July, 2019.

In 2018, the Fund provided A$6.5 million (~US$4.5 million) funding across ten projects that are contributing to Australia's growing cyber security ecosystem. In 2019, an additional A$8.5 million (~US$6 million) is available and will be awarded to industry-led projects that deliver on the goals of AustCyber's Cyber Security Sector Competitiveness Plan.

Virginian companies could capitalize on this funding initiative by partnering with local Australian companies with complementary technology solutions or services. To note, lead applicants must have an Australian Business Number (ABN) and be an entity incorporated in Australia, however joint applications are acceptable providing the lead applicant is the main project driver.

Interested companies are encouraged to review the Criteria and Guidelines and Application Process in further detail.

INDUSTRY OPPORTUNITIES

Critical Infrastructure

Critical Infrastructure and systems comprise the essential services across all major sectors including banking and finance, defense, communications, energy, resources, health, transport and water. Therefore, safeguarding Australia's critical infrastructure from any disruptive threats is a matter of **national interest**.

As internet connectivity, information and communications technology and industrial control systems are increasingly used to support its delivery, critical infrastructure is increasingly a target of cyber adversaries attempting to disrupt or destroy assets of national importance.

In response to growing cyber security threats, the Australian Government established the Critical Infrastructure Centre in January 2017 to safeguard Australia from foreign interference and security risks, including sabotage, espionage, coercion.

The Centre safeguards Australia across all eight critical infrastructure sectors through the following initiatives:

- ✓ Conducting whole-of-government **national security risk assessments**;
- ✓ Developing **risk management strategies** and providing advice;
- ✓ **Supporting compliance**;
- ✓ Providing **best practice guidance** to owners and operators of critical infrastructure;
- ✓ Assisting state and territory government, regulators and owners to **manage risk and build resilience**; and
- ✓ Complementing the Foreign Investment Review Board (FIRB) by providing early national security advice to inform the Treasurer's decision on **foreign investment proposals**.

In July 2018, the Critical Infrastructure Centre enacted the *Security of Critical Infrastructure Act 2018* to manage complex and evolving national security risks posed by foreign involvement in Australia's critical infrastructure. The Act will provide the government with a more detailed Register of Critical Infrastructure Assets, and the power to obtain more detailed information or to direct an owner / operator of critical infrastructure to undertake certain activities in order to mitigate against a national security risk.

Health Care

The Australian health care sector presents a high level of opportunity to Virginian companies with expertise in the protection of health data and systems. Australia spent close to **A$181 billion** (~US$126 billion) on health in 2016-17, equating to **~10% of overall economic activity**. **69% of this health spending was funded by the Australian Government and state/territory governments** (A$70 billion (~US$40 billion) and $50 billion (~US$35 billion) respectively). Non-government spending (private health care, health insurance, individuals) accounted for the remaining 31% of spending.

There are currently ~695 public hospitals and ~630 private hospitals across Australia. As such, both public and private health care providers (e.g. Epworth Healthcare, Ramsay Health Care,

Healthscope etc.) represent potential end customers for Virginian exporters offering cyber security services, hardware, and software solutions.

As one of the most data rich sectors vulnerable to ransomware and other cyber-attacks, the health care sector faces the unique challenge of balancing security with accessibility to patient records and delivering a patient-centric approach to health care.

The Office of the Australian Information Commissioner's (OAIC) most recent *Notifiable Data Breaches Quarterly Statistics Report* highlighted that private health service providers reported the most data breaches in the period from 1 October – 31 December 2018, accounting for 54 of the 262 breach notifications received.

Further, an audit conducted in May 2019 found patient data stored in Victoria's public health system to be highly vulnerable to cyber-attacks, noting that several health agencies have low-risk awareness of potential risks and flaws in the security of patient data and hospital services.

In response to increasing cyber threats on the sector, the Australian Digital Health Agency (ADHA), which is responsible for delivering national digital health services and systems in Australia, established a dedicated Digital Health Cyber Security Centre in 2017.

The Centre is intended to provide a range of cyber security capabilities to strengthen the security of Australia's digital health systems and services (e.g. the My Health Record electronic health record system), as well as to promote increased security awareness and maturity across the digital health sector.

These goals will be achieved through the Centre's **key initiatives**:

- ✓ Establishing **partnerships** with a range of national and international cyber security organizations across government and the private sector, in order to improve knowledge of cyber threats and leveraged shared experience and best practices;
- ✓ The development of cyber security **guidance materials** and threat intelligence information specific to the digital health sector;
- ✓ Undertaking **operational security activities** and incorporating security in the design of national digital health systems;
- ✓ Coordinating **security incident response activities** related to national digital health systems or services operated by/for the ADHA;
- ✓ Assisting the Australian Cyber Security Centre (ACSC) by **coordinating the healthcare sector response** in the event of a major cyber security incident; and
- ✓ Developing a **toolkit** to assist healthcare businesses and professionals to select secure IT products and services, in conjunction with the ADHA's Information Security Guide and Stay Smart Online service.

Defense

Cyber security is a significant priority for the Australian Government Department of Defense, and is continuing to grow in importance as the volume and sophistication of potential cyber threats increase. Defense has one of the largest ICT networks in Australia, as it supports a wide range of military, administrative and management capabilities. Under the ICT Investment Plan, Defense is expected to spend **~A$623 million (~US$435m) on ICT in 2018-19**, and this figure is expected to increase to **~A$950 million (~US$664m) in 2019-20**.

The Chief Information Officer Group (CIOG) within the Department of Defense leads the integrated design, cost effective delivery, and sustained operation of Defense's Single Information Environment (SIE) to support military and business operations.

The SIE encompasses information, computing and communications infrastructure and management systems, which are core to Defense's intelligence, surveillance, reconnaissance, communications, information warfare, command and management functions.

Ultimately, the CIOG is responsible for ensuring that the Department of Defense has a dependable, secure and integrated information environment that is capable of supporting operational and management requirements.

Defense ICT security personnel work closely with the CIOG, the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) to understand current threats and implement measures to prevent, detect and respond to targeted cyber intrusions (e.g. ransomware, spear phishing emails etc.).

In January 2018, Defense established two new cyber units to work alongside the ASD: SIGINT (signals intelligence unit) and Cyber Command. These recently announced units stress Defense's growing focus on security measures and proactively identifying and mitigating cyber risks.

Virginian companies interested in working as contractors to the Australian Department of Defense are encouraged to undertake the following steps in order to best position themselves as potential suppliers from a cyber security perspective:

- ✓ Implementing and **demonstrating compliance** with the mandatory *Strategies to Mitigate Cyber Security Incidents* published by the ASD in the *Australian Government Information Security Manual*;
- ✓ If sub-contractors are engaged, contractors must ensure that they establish **prescriptive cyber security requirements** and retain some level of **control over the supply chain** by gathering evidence of compliance with these established terms; and
- ✓ Virginian companies should proactively provide information, undergo up-front risk assessments and obtain cyber security assurances in order to **preemptively address any potential risks associated with contracting as an overseas supplier**.

Banking, Financial Services & Insurance (BFSI)

Firms within the Banking, Financial Services & Insurance (BFSI) sector are key targets for data breaches due to the significant amount of sensitive client information they store, which is commonly used in cases of tax, superannuation and financial fraud and identity theft.

To protect client data, firms must take adequate precautions through the development of a **secure, vigilant and resilient cyber risk program**. This may include:

- ✓ Focusing protection around the most risk-sensitive assets, e.g. critical infrastructure, applications, data and specialized control systems;
- ✓ Addressing weak points along the end-to-end business process and larger services and transaction chains;
- ✓ Having the capacity to rapidly contain damage and mobilize the diverse resources needed to minimize impacts such as business disruption, reputation and brand damage; and
- ✓ Investing in both traditional technology-based disaster recovery capabilities as well as complete crisis management capabilities.

Recent evidence of a heightened focus on cyber resilience, with regulators and large financial institutions investing in solutions to strengthen cyber security, indicates a growing number of opportunities for Virginian exporters. Examples of initiatives implemented by actors within Australia's BFSI sector over the past twelve months include:

- ✓ The Reserve Bank of Australia (RBA) has been prioritizing cyber security in the supervision of Australia's financial market infrastructures (FMIs), also reviewing ASX companies against international cyber resilience guidelines;

- ✓ The Australian Securities and Investments Commission (ASIC) has been strategically reviewing the cyber resilience of financial sector firms it regulates; and

- ✓ SWIFT has introduced a program to establish mandatory controls for security, guidelines for monitoring network breaches, and a protocol for sharing information on attacks.

KEY PLAYERS

INTERNATIONAL COMPANIES

According to AustCyber, international providers meet a significant portion of the current demand for cyber security products and services in Australia.

AustCyber estimates suggest that Australia imported ~A$1.6 billion (~US$1.1 billion) of cyber security products and services in 2017, in comparison to ~A$350 million (~US$245 million) in exports.

Key international companies operating in the Australian market, the majority of which are headquartered in the US, include:

LOCAL COMPANIES

Start-ups

Australia's cyber start-up scene is still immature, and some innovative new firms are being met with conservatism from larger corporations.

Australia currently has only one cyber security focused start-up accelerator, CyRise. However, as the sector is predicted to grow rapidly and evolve to meet the demands of new cyber threats, the Australian Financial Review is optimistic that larger local cyber companies will emerge.

Examples of Australian cyber security start-ups include:

Software, Hardware & Managed Security Service Providers (MSSPs)

There are currently no local companies among the 15 largest software providers (by value) in the Australian cyber security market. The combined market share of local companies is estimated by AustCyber to be less than 5%.

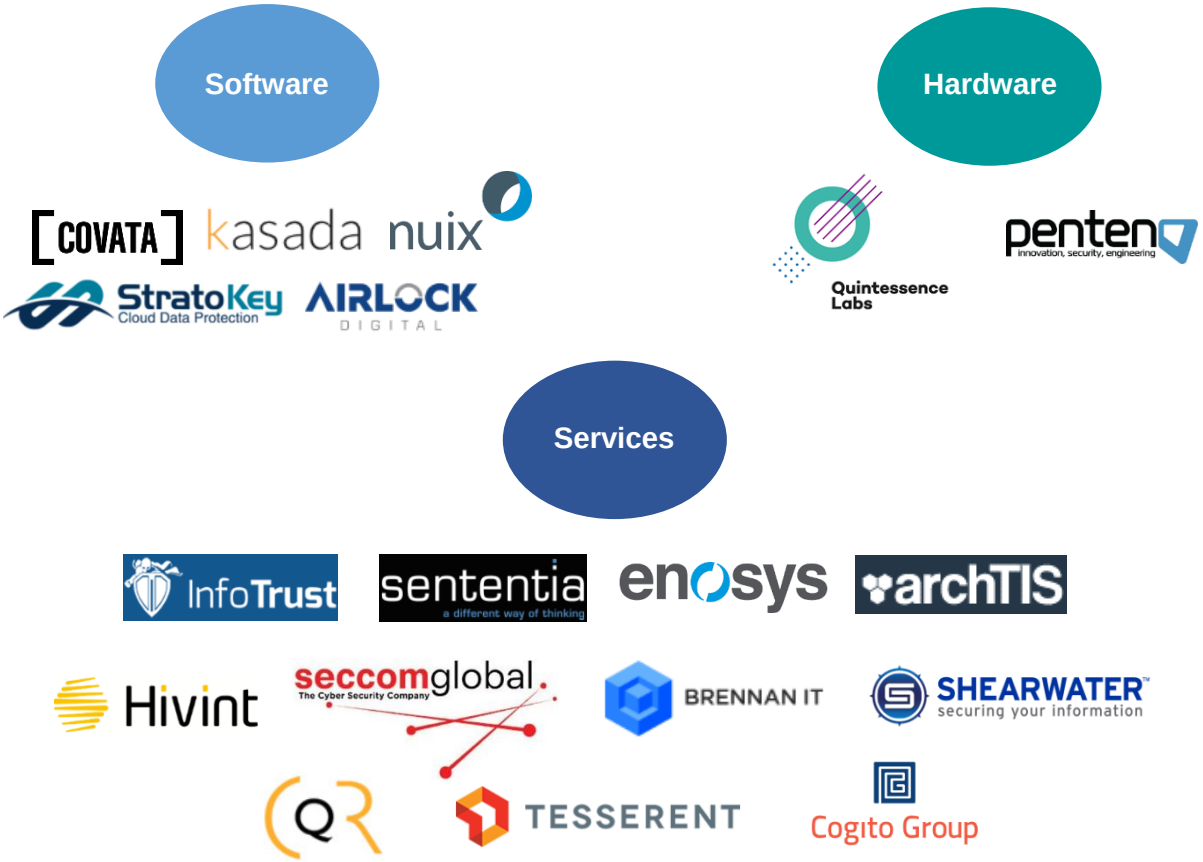
According to AustCyber, Australian companies are most competitive in the software and services segments. The representation of Australian companies is **strongest in the services segment**, where Australian companies account for ~25% of market share.

MSSPs offer organizations complete managed security services through a 24/7 security operations center (SOC) and security information and event management (SIEM) software, in order to provide real-time analysis of threats, generate alerts and provide advice on and carry out remedial action.

TechSci Research estimates that the Australian managed security services (MSS) market will grow at over **15% CAGR until 2024**. This is due to increasing demand for services related to cloud security, data security, forensic services, security analytics and risk assessment among Australian end users.

The increased uptake of cloud computing, the popularity of bring-your-own-device and the shortage of cyber skills in the face of an ever-evolving threat landscape, is also contributing to the growth of the cyber security sector and the emergence of new companies.

Key local players, which represent potential competitors to Virginian exporters, include:



There is also evidence of Australian companies that have expanded globally, and are now headquartered in the US. Examples include:

FEDERAL GOVERNMENT AGENCIES / NETWORKS

Australian Signals Directorate (ASD)

www.asd.gov.au

As Australia's national cryptology agency, the Australian Signals Directorate (ASD) is a vital part of Australia's national security community. It supports the Australian Government and Australian Defence Force (ADF) by working across the full spectrum of operations required of contemporary signals and security agencies, including intelligence, **cyber security**, and offensive operations. The ASD is headed by the Director-General (currently Mike Burgess), who is responsible to the Minister for Defense.

The three main goals of the ASD are to:

- ✓ **Inform** through covertly accessing information not publicly available;
- ✓ **Protect** by comprehensively understanding cyber threats and providing leading advice and proactive assistance so that governments, industry and the community are able to effectively respond to and better manage cyber security risks; and
- ✓ **Disrupt** by delivering high-impact, full-spectrum offensive cyber operations that support Australian Government priorities, including supporting military operations, law enforcement & criminal intelligence activity against cyber criminals, and responding to serious cyber incidents against Australian networks.

These aims are achieved through forensic analysis, intrusion detection, offensive cyber operations, the analysis of communication systems and foreign signals intelligence etc.

Australian Cyber Security Centre (ACSC)

www.cyber.gov.au

The Australian Cyber Security Centre (ACSC) sits within the ASD and provides information and advice on cyber security threats, initiates partnerships programs, and produces the Australian Government Information Security Manual (ISM).

The purpose of the ISM is to assist organizations to use their risk management framework in order to protect information and systems from cyber threats. The guidelines provided in the ISM cover both governance and technical concepts related to the protection of an organizations' information and systems, and are therefore intended for Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), cyber security professionals and IT managers.
The ACSC constantly monitors for cyber security threats from a range of local and global sources, including through public and private sector Computer Emergency Response Teams (CERTs) on a global scale. Registered partners of the ACSC automatically receive threat

intelligence, consisting of actionable and timely information that enables the prioritisation and effective implementation of countermeasures in response to cyber threats.

The ACSC also manages several programs and initiatives that drive collaboration between government, industry and research partners. For example, the ACSC Joint Cyber Security Centre (JCSC) program provides a range of services and support, with centres in most of Australia's capital cities.

Another program open to ACSC partners is the Australian Internet Security Initiative (AISI), which operates as a public-private partnership where Australian internet providers voluntarily work with the ACSC to protect their customers from potential cyber security threats. The program provides internet providers with data that is used to identify and inform users about malicious software (malware) infections and service vulnerabilities, and provide information on how they can be remedied.

Aside from involvement in ACSC programs, partners of the centre are able to access timely and sensitive information such as cyber threat intelligence and information on incidents, threats and risks, develop collaborative solutions to cyber security risks, and attend events, workshops and presentations on the Australian cyber security sector.

ACSC partnership is available to:

- ✓ Businesses that hold an Australian Business Number (ABN) and maintain IT security personnel in Australia that are able to act on operational cyber security / technology information;
- ✓ Australian government agencies (federal, state & territory) with a defined role or key interest in Australia's cyber security arrangements;
- ✓ Security vendors and consulting firms willing to contribute their cyber security capabilities to the Joint Cyber Security Centre Program (JCSC) on a not-for-profit basis; and
- ✓ Academic, research and not-for-profit institutions.

Australian Cybercrime Online Reporting Network (ACORN)

www.acorn.gov.au

The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of Australia's federal, state and territory governments, designed to make it easier for the public to report cybercrime, and to gain a better understanding of the cybercrime affecting Australians. ACORN provides advice on common types of cybercrime (e.g. hacking, online scams, online fraud, identity theft, computer system attacks) and enables the public to securely report instances of cybercrime online. ACORN is a key initiative under the government's National Plan to Combat Cybercrime, which outlines how Australian government agencies are working together to protect Australia from cybercriminals.

Trusted Information Sharing Network (TISN)

www.tisn.gov.au

Established by the Australian Government in 2003, the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience is Australia's primary national engagement mechanism for business-government information sharing and resilience building initiatives for critical infrastructure.

The TISN comprises eight sector groups (covering banking, finance, communications, energy etc.) overseen by the Critical Infrastructure Advisory Council that enable owners and operators to share information on threats and vulnerabilities and to collaborate within and across sectors to mitigate risk and boost resilience.

The TISN also supports the Australian Government's Cyber Security Strategy, as secure information and communications technologies underpin the operation of critical infrastructure.

STATE / TERRITORY GOVERNMENT AGENCIES & NETWORKS

New South Wales (NSW)

Cyber Security NSW

In May 2019, the NSW Government launched a purpose-built cyber security office that will operate within the NSW Department of Customer Service from July 1, 2019 under the leadership of Tony Chapman, Chief Cyber Security Officer.

The division will focus on digital transformation, improving customer service, risk management and awareness to support greater resilience to cyber security threats.

Cyber Security NSW will also work on enhancing whole-of-government cyber security capabilities and standards, and will work alongside the Information and Privacy Commission on security, privacy and the availability of systems and services.

NSW Cyber Security Network (NSWCSN)

www.nswcybersecuritynetwork.com.au

The NSW Cyber Security Network (NSWCSN) is a NSW Government initiative funded by the NSW State Government and seven member universities. The network was announced in February 2018 as a A$2 million (~US$1.4 million) investment to bolster NSW's cyber security research and development capability and harness the state's growing cyber security industry.

The purpose of the NSWCSN is to facilitate collaboration between universities specializing in cyber-related research, promote their capabilities, and to support their connection with industry in order to position NSW as a leader in cyber security.

The NSWCSN promotes the R&D capabilities of its member universities (specialized in research areas such as machine learning, cloud security, data analytics, security assurance, cryptography, application security, trust and governance) in order to improve outcomes for industry and Government.

Other initiatives developed by the NSWCSN include a workforce development program for cyber professionals and the NSW Cyber Security Innovation Node, a partnership between the NSW Government and AustCyber.

Queensland (QLD)

Queensland Government Chief Information Office (QGCIO) Cyber Security Unit

www.qgcio.qld.gov.au

In 2016, the Queensland Government committed A$12.5 million (~US$8.7 million) in funding towards the establishment of a dedicated whole-of-government Cyber Security Unit in order to develop a coordinated approach to mitigate cyber threats, protect government information technology systems and to manage major cyber security incidents.

The Queensland Government has since established a Cyber Security Steering Committee comprising senior executives to oversee and review a range of government protections and programs, including enhancing the Queensland Government's internet gateway protection services.

The Unit also supports government agencies by increasing the visibility and awareness of current cyber security risks in order to encourage informed business decisions.

Victoria (VIC)

In 2016, the Victorian Government released the Cyber Security Strategy 2016 - 2020 and committed to investing A$17.6 million (~US$12.3 million) over four years towards its implementation. The government also appointed John O'Driscoll as Victoria's first Chief Information Security Officer (CISO) in October, 2017.

Under the strategy, the Victorian Government CISO is responsible for coordinating an efficient and effective whole-of-government approach to security. This includes the creation of cyber services, capabilities, reporting, executive engagement and information dissemination across all government agencies in Victoria, the majority of which are unable to achieve and sustain appropriate levels of cyber resilience on their own.

Government funding will also be used to improve detection and prevention capabilities and responses to cyber-attacks on Victorian Government IT systems, thereby protecting the delivery of public services across the entire government.

Victoria's commitment to cyber security research and capability improvement is demonstrated by their investment in the local node to AustCyber, the establishment of the Data61 Cyber Security Innovation Hub, and the Oceania Cyber Security Center.

INDUSTRY ASSOCIATIONS

AustCyber

www.austcyber.com

AustCyber was established in 2017 as an independent, not-for-profit organisation. AustCyber is funded by federal government grants and forms part of the Australian government's Industry Growth Centre Initiative which was established through the National Innovation and Science Agenda, and is an important part of Australia's Cyber Security Strategy as a key enabler for cyber security research, development and innovation.

AustCyber's mission is to support the development of a vibrant, globally competitive Australian cyber security sector. The organisations strategic objectives are to:

- ✓ Grow an Australian cyber security ecosystem;
- ✓ Export Australia's cyber security to the world; and
- ✓ Make Australia the leading centre for cyber education.

AustCyber works to align research and innovation related activities across the private sector, research communities, academia and government. The organisation also works internationally with a range of partners to develop export pathways for Australian solutions and capability, and to tap into global cyber security hubs around the world.

AustCyber's programme of activities is underpinned by the Sector Competitiveness Plan and Industry Roadmap, which outlines the opportunity for Australia's cyber security sector to support growth across the whole economy. The organisations current priorities are to:

- ✓ Establish a national network of AustCyber nodes;
- ✓ Build a pipeline of skilled cyber security professionals;
- ✓ Support cyber security solutions from initial set up to export; and
- ✓ Manage a Projects Fund for industry-led projects.

Australian Information Security Association

www.aisa.org.au

Established in 1999, the Australian Information Security Association (AISA) is a national not-for-profit organisation that champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the security of the Australian public, business and government.

AISA was established to provide leadership for the development, promotion and improvement of cyber security through advocacy, diversity, education and organisational excellence. The organisation currently has a base of over 3,500 individual and corporate members from all domains of the information security industry.

Initiatives carried out by AISA include:

- ✓ Facilitating and evolving best practice data and information security practices and systems, including research & development;

- ✓ Assisting organisations to reduce identity theft, financial crimes, fraud & unauthorised access to information systems;
- ✓ Educating individuals and organisations about information security issues and the risks and dangers of cyber-attacks and data theft; and
- ✓ Advising government on the development of information security policy, law and legislation.

RESEARCH CENTRES

Cyber Security Cooperative Research Centre (CSCRC)

www.cybersecuritycrc.org.au

The CSCRC was established in April 2018 as part of the Australian Government's Cooperative Research Centres (CRC) Program, and has been granted A$50 million (~US$35 million) funding over the next six years.

The centre is focused on delivering industry-driven cyber security research outcomes that address real-world cyber security problems with innovative solutions through its mission:

"To be an independent and collaborative centre where industry, government and research partners work together to create new products, services and systems that deliver a secure and resilient national cyber security capability, and enhance cyber expertise for the nation, making Australia a safer place to do business."

To achieve this mission, the CSCRC is aiming to:

- ✓ Improve collaboration between industry and universities to grow Australia's cyber security sector capabilities;
- ✓ Undertake a key role in cyber security advocacy by providing easy to understand, evidence-based commentary on cyber security issues;
- ✓ Produce research that impacts how government, businesses and Australian effectively manage cyber security risk (the focus of current research programs is 'Critical Infrastructure Security' and 'Cyber Security as a Service'.

Oceania Cyber Security Centre (OCSC)

http://oceaniacybersecuritycentre.businesscatalyst.com

The OCSC is a collaboration of eight Victorian universities (Monash, Melbourne, Deakin, Federation, RMIT, Swinburne, La Trobe, Victoria) that is based in Melbourne and supported by the Victorian Government.

The centre's aim is to engage with industry and government partners to provide advice on current and future security threats, develop new technology and create commercialisation opportunities, and to train staff and students on the latest techniques for protecting security.

The OCSC's main initiatives are centred on: Critical Infrastructure and the Internet of Things; Verification; Social Media; Advanced Cryptography; Big Data; Network Security; and Automation and Industrial Control Systems.

LOCAL LEGISLATION & REGULATORS

Virginian companies exploring opportunities to do business in Australia are encouraged to take the following local legislative requirements related to cyber security into consideration.

The Australian Government's Office of the Australian Information Commissioner (OAIC) is responsible for overseeing:

- ✓ The *Privacy Act 1988*;
- ✓ The Notifiable Data Breaches Scheme;
- ✓ The *Freedom of Information (FOI) Act 1982*; and
- ✓ Government information policy functions.

PRIVACY ACT 1988

In Australia, the Privacy Act regulates any data breach or cyber security incident involving **personal information** (i.e. information or opinion that identifies or could be 'reasonably used' to identify or locate an individual). The Act regulates:

- ✓ Most government agencies;
- ✓ All private and not-for-profit organizations with annual turnover over A$3 million (~US$2.1 million); and
- ✓ All small businesses that store personal information (e.g. health service providers).

Under the Act, these organizations are required to comply with the Australian Privacy Principles (APPs), a set of thirteen (13) legally binding principles related to the handling, use and management of personal information. The APPs cover:

- ✓ The open and transparent management of personal information;
- ✓ The collection of solicited personal information and receipt of unsolicited personal information;
- ✓ The option for individuals to transact anonymously or use a pseudonym;
- ✓ How personal information can be used and disclosed (including overseas);
- ✓ Maintaining the quality of personal information;
- ✓ Keeping personal information secure; and
- ✓ The right for individuals to access and correct their personal information.

NOTIFIABLE DATA BREACHES SCHEME (NDB)

In February 2018, the OAIC implemented the Notifiable Data Breaches (NDB) Scheme, a regulatory regime designed to manage and improve cyber security accountability in Australia that applies to all organizations with existing personal information security obligations under the Privacy Act.

Under the Scheme, it is compulsory for organizations to assess suspected data breaches and to notify the OAIC, the Australian Information Commissioner and any affected individuals when a data breach occurs that is likely to result in 'serious' harm to any individual affected.

The OAIC specifies four high-priority data categories that are 'more likely to cause an individual serious harm if compromised'.
These include:

- ✓ Sensitive information (e.g. information about an individuals' health);
- ✓ Medicare card, driver's license and passport details;
- ✓ Financial information; and
- ✓ Multiple data points about an individual.

These types of data are commonly targeted by cybercriminals, and fit with current trends indicating that cybercrime is being driven by identify fraud leveraging stolen personal data.

INDUSTRY-SPECIFIC CYBER SECURITY REGULATIONS

Cyber security regulations specific to certain industry sectors is also starting to emerge, for example in the telecommunications and banking & insurance industries.

Telecommunications

The *Telecommunications and Other Legislation Amendment Act 2017*, known as the Telecommunication Sector Security Reforms (TSSR), are a series of reforms and broader regulatory framework implemented by the Critical Infrastructure Centre that are designed to better manage national security risks (e.g. espionage, sabotage, foreign interference etc.) to Australia's telecommunications networks and facilities.

The TSSR came into effect in September 2018 and contains the following key elements:

- ✓ **Security Obligation**: All carriers, carriage service providers and intermediaries are required to 'do their best' to protect networks and facilities from unauthorized access and interference and to maintain effective supervision & control over their networks;

- ✓ **Notification Obligation**: Carriers/ service providers will be required to notify government of planned changes to their systems/services that could compromise their capacity to comply with security obligations;

- ✓ **Information Gathering Power**: The Secretary of the Department of Home Affairs has the power to obtain information and monitor and investigate compliance with security obligations; and

- ✓ **Directions Power**: The Home Affairs Minister has the power to direct carriers/ service providers to undertake certain activities in order to protect networks and facilities from national security risks.

Banking & Insurance

The Australian Prudential Regulation Authority (APRA) is the prudential regulator of the financial services industry that oversees Australian banks, credit unions, insurance and reinsurance companies, building societies and the superannuation industry.

In November 2018, APRA released the final version of its new prudential standard focused on information security management, the Prudential Standard CPS 234: Information Security.

The new standard is aimed at improving resilience against information security incidents (including cyber-attacks), and their ability to respond quickly and effectively if faced with a security breach. Under the standard, APRA-regulated entities are required to:

- ✓ Clearly define information-security related roles and responsibilities;
- ✓ Maintain an information security capability equal to the size of information assets;
- ✓ Implement controls to protect information assets and undertake regular testing; and
- ✓ Notify APRA of any material information security incidents.

APRA is fast-tracking the implementation of CPS 234, with all regulated entities expected to meet the new requirements by 1 July 2019.

To assist entities to comply with the new standard, APRA has also published a draft version of the updated Prudential Practice Guide – CPG 234 Information Security.

MARKET ENTRY STRATEGY

RECOMMENDATIONS

Virginian companies interested in exploring opportunities in Australia's cyber security sector are encouraged to undertake the following key steps:

- ✓ **Understand the market and customer demand;**
- ✓ **Select the most suitable partner and/or establish an office / local presence; and**
- ✓ **Provide ongoing support in the market.**

Understanding Market & Customer Demand

In order to gain a deeper understanding of demand in the Australian market for a specific product or service, Virginian companies are encouraged to:

- ✓ Engage with key **industry associations** for cyber security in Australia and subscribe to **industry publications** to stay up to date on recent developments and current issues (see following section for details).

- ✓ Participate in a **market visit** in order to gather additional market intelligence and meet with prospective partners in person. This visit could be undertaken individually, or as part of a group trade mission, such as the VEDP Trade Mission to Australia in October 2019, which will align with one of the key industry sector events – the Australian Cyber Conference 2019 (further details below).

Establishing a Presence in the Australian Market

Virginian companies wishing to establish a presence in the Australian market following an initial market visit are encouraged to explore the following potential options, which include appointing a local distributor / partner, setting up a local office, acquiring a local company, or setting up a foreign joint venture/strategic alliance.

- ✓ **Setting up a local office or branch** offers customers a reassurance of your company's commitment to the local market, as well as more control of the business operations and marketing. Some drawbacks include higher risk and set up capital, initial lack of business contacts, and lack of established reputation in Australia.
- ✓ **Appointing a local distributor / integration partner** offering similar or complementary products offers the benefits of lower initial investment, established local contacts and a faster time frame for market entry. Some drawbacks include trust issues (regarding liability), lack of control of business operations and possible performance issues if no sales milestones are set in place.
- ✓ **Acquiring a local company** – May take less time to access and penetrate the market as the company would have an existing distribution network in place. The drawback would be a **large capital investment**, and possible slower post-merger integration.
- ✓ **Setting up a Foreign Joint Venture/Strategic Alliance** – Virginian companies could also consider forming a joint venture, or strategic alliance with a local Australian company. The advantage would be possible faster market entry. However, potential risks could be differing on goals and objectives and also lack of total control of management.

The decision of which market entry route to undertake will ultimately come down to the short, medium and long-term business objectives of the specific company. Our general recommendation for Virginian companies wishing to explore opportunities in the Australian cyber security sector is to appoint a **local technology partner.**

Supplying to Public & Private Sectors

The procurement process may vary considerably within different industries, as well as between the private and public sectors.

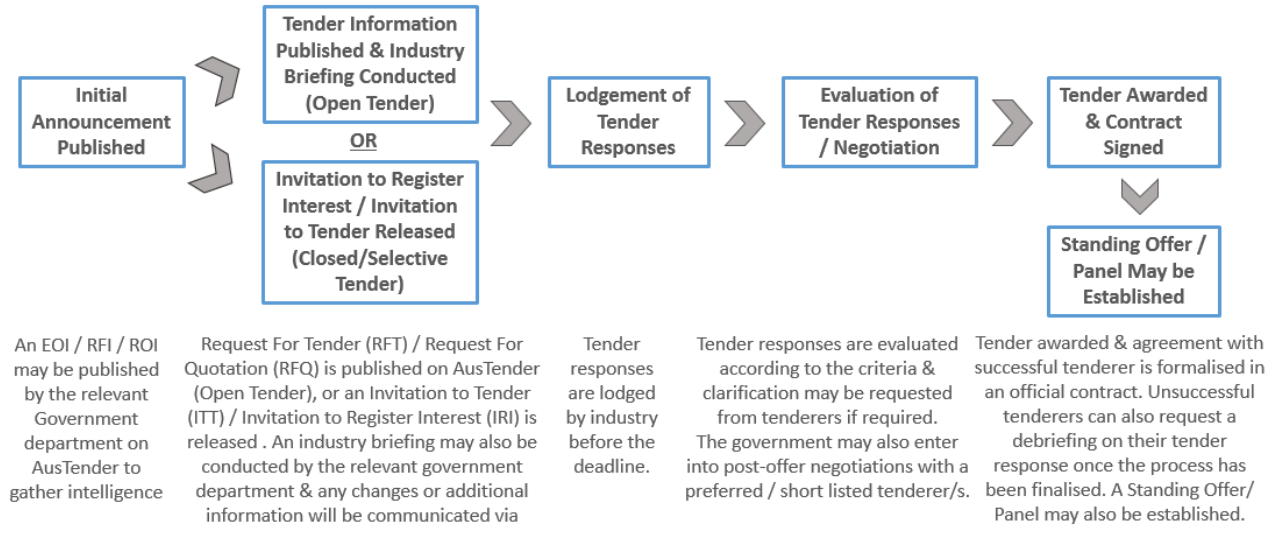
The process of supplying cyber security products and services will differ if potential end customers are predominantly in the public sector (i.e. Defense), the private sector (i.e. BFSI), or a combination of both (i.e. health care).

For some sectors such as health care and education, Virginian exporters have the potential to supply to both the Australian federal government and state/territory governments, as both levels are involved in the funding, procurement and delivery of certain services.

The 'Selling to Government' guide published by the Department of Finance provides potential suppliers with all relevant information related to the bidding process, covering:

- ✓ **Identifying Opportunities** to Sell to Government;
- ✓ **Responding to an Approach to Market** (ATM); and
- ✓ Government Procurement **Rules & Processes.**

The **typical bidding process for government contracts** is as follows:



Virginian companies interested in supplying to the Australian federal government and/or state/territory governments are encouraged to subscribe to AusTender, the Australian government online tendering platform, to receive up to date information on current business opportunities, annual procurement plans, multi-use lists and contracts relevant to cyber security.

Virginian exporters are also encouraged to register to receive email notifications from the following state/territory procurement websites:

- ✓ Australian Capital Territory (ACT): Tenders ACT
- ✓ New South Wales (NSW): NSW eTendering
- ✓ Northern Territory (NT): NT Quotations and Tenders Online
- ✓ Queensland (QLD): QLD QTenders
- ✓ South Australia (SA): SA Tenders and Contracts
- ✓ Tasmania (TAS): Tasmanian Government Tenders
- ✓ Victoria (VIC): Buying For Victoria
- ✓ Western Australia (WA): Tenders WA

Companies interested in supplying to the **private sector** are encouraged to conduct research and identify specific organizations demonstrating a commitment to invest in cyber security solutions/services, and may therefore represent potential end customers.

The majority of large private organizations have their own procurement/sourcing department that manages the tendering process.

Ideally, Virginian companies should seek to identify and appoint a local partner that has established relationships with key stakeholders in both the public and private sectors, as well as the capacity to invest time into growing a brand in Australia and provide ongoing support to potential end customers.

INDUSTRY PUBLICATIONS

Australian Cyber Security Magazine

www.australiancybersecuritymagazine.com.au

Executive Editor: Chris Cubbage
Tel: +61 (0) 432 743 261
Email: promoteme@mysecuritymedia.com

The Australian Cyber Security Magazine is published by the Australian Information Security Association (AISA) in partnership with My Security Media. The magazine is focused on AISA's ~3,500 members, and forms part of the association's national cyber security awareness and membership communication platform.

View the current issue online.

Australian Security Magazine

www.australiansecuritymagazine.com.au

Australian Security Magazine is a bi-monthly government and corporate security magazine that is distributed free of charge to major players in Australia's security industry, and also sold to the Australian public. The publication incorporates investigative journalism, editorial features, and current news, trends and events relevant to security professionals. It is supplemented by the Asia Pacific Security Magazine, a free publication focusing on major events in the Asia Pacific region.

CRN Magazine

www.crn.com.au

Editor: Michael Jenkin
Tel: +61 (0) 2 9901 6395
Email: mjenkin@crn.com.au

CRN Australia is a central source of news and business insight, analysis and strategic information for IT resellers, systems integrators, managed service providers, IT solutions companies, distributors and vendors. The magazine looks in-depth at emerging issues and developments in the IT, digital and cyber security sectors.

View the current issue online.

INDUSTRY EVENTS

2019 Security Exhibition & Conference

www.securityexpo.com.au
Dates: 24 – 26 July, 2019
Location: International Convention Centre, Darling Harbour, Sydney, New South wales

The Security Exhibition & Conference, hosted in partnership with the Australian Security Industry Association Limited (ASIAL), is one of the largest commercial events for the Australian security industry, connecting the entire supply chain of manufacturers, distributors, security professionals and end users to create business opportunities.

The theme of the 2019 ASIAL Security Conference, 'Building Resilience to Combat Changing Security Threats', will feature a program of local and international experts and academics who will address how to strengthen capabilities, manage risk, and utilize emerging technologies and innovations in a digital future.

Cyber Security in Government

www.terrapinn.com/exhibition/cyber-security-in-government
Dates: 6 – 7 August, 2019
Location: National Convention Centre, Canberra, Australian Capital Territory

The Cyber Security in Government Conference is a two-day event co-located within Australia's largest annual government ICT events, Tech in Gov. The event brings together private sectors industry leaders and CISOs, CIOs, cyber security, risk and fraud professionals from Federal and State government, to discuss the latest technologies and strategies for managing cyber risk. Areas of discussion include cyber human factors, cyber workforce, cyber compliance, privacy and data breach regulations, cyber-crime etc.

Australian Cyber Conference 2019

www.cyberconference.com.au
Dates: 7 – 9 October, 2019
Location: Melbourne Convention & Exhibition Centre, Melbourne, Victoria

The Australian Cyber Conference 2019 will provide an opportunity for business leaders to network with cyber security experts and to better understand how to manage current threats, and identify and prepare to meet emerging challenges. The conference will feature an interactive format of workshops, plenary sessions and networking events.

Delegates range from company directors and managers to risk professionals, software architects and technical security specialists, from a broad range of industries such as education, finance, government, healthcare, manufacturing, mining, transport, utilities etc.

APPENDIX

RECENT EXAMPLES OF CYBER ATTACKS / DATA BREACHES

Department of Parliamentary Services

As a result of a malicious cyber-attack, thought to have been carried out by a state actor, in February Australian parliamentarians and their staff were forced to reset passwords in order to protect their network, affecting 4,000 users.

Toyota Australia

In February 2019 Toyota Australia suffered an 'attempted cyber-attack' which took out its email and other online systems.

Datacom, a New Zealand based ICT company that supplies infrastructure and support services to Toyota Australia advised that Toyota hosts its own infrastructure, and 'does not use Datacoms cloud platforms or datacenters'. Datacom also doesn't supply security services to Toyota under their outsourcing agreement, however is assisting with the recovery process.

Melbourne Heart Group (located at Melbourne Cabrini Hospital)

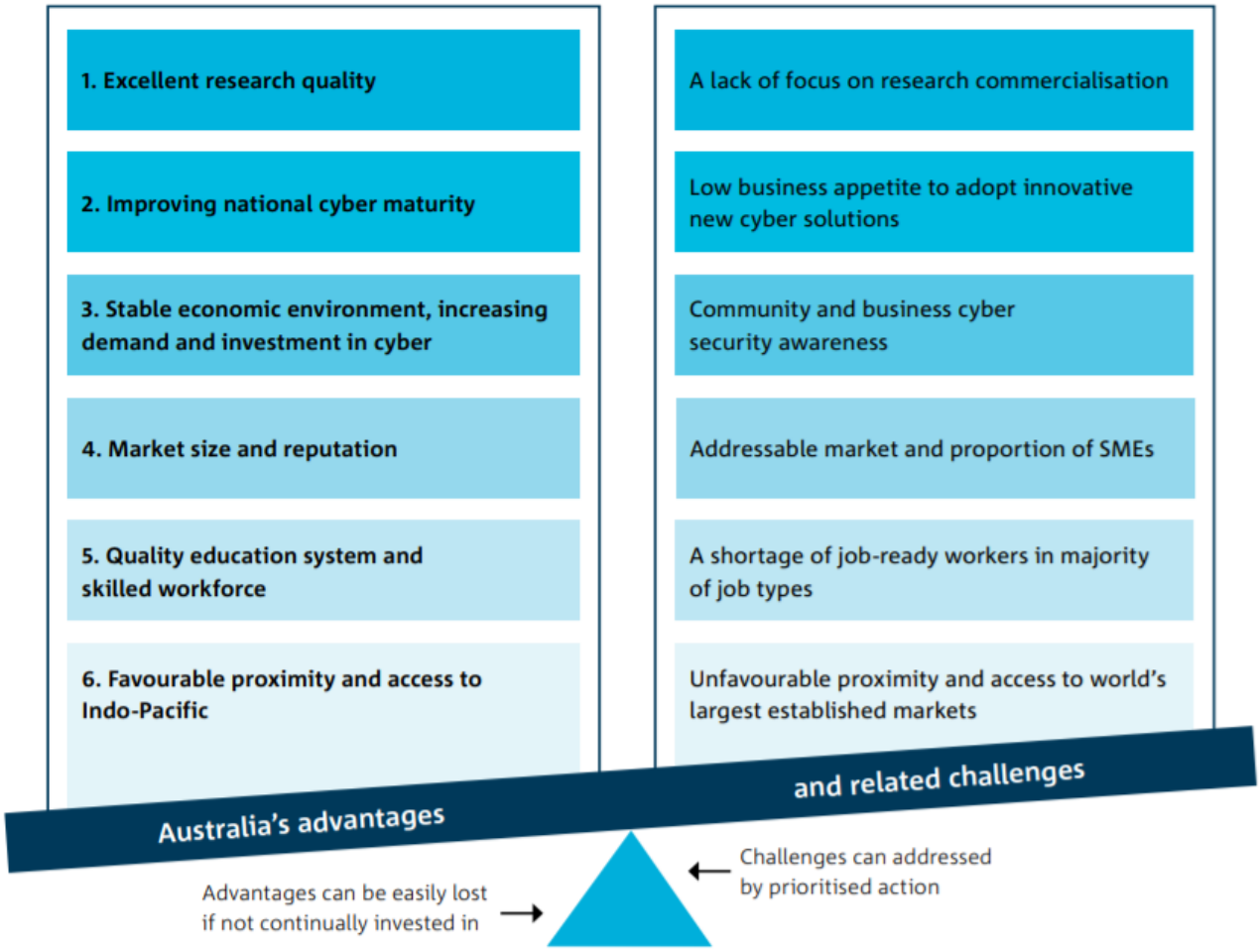
In February 2019, a suspected cybercrime syndicate accessed the medical files of 15,000 patients at Melbourne Heart Group, based inside Melbourne Cabrini Hospital. Medical professionals were unable to access some patient records for up to three weeks.

Hospital Chief Executive advised that data and other information systems are owned and managed by the specialists, not Cabrini. Further distancing the attack from the hospital, the Chief Executive also advised that the specialists are not employees of the hospital.

Bank of Queensland

On 11 March, 2019 it was reported that the Bank of Queensland was the victim of a personal data breach by a third-party provider – Landmark White Limited, a fund management company and provider of property evaluations.

ADVANTAGES AND CHALLENGES IN AUSTRALIA'S CYBER SECURITY SECTOR



Source: CSIRO Futures/AustCyber