CYBERSECURITY IN AUSTRALIA

CYBERSECURITY OVERVIEW

- The Australian Government has identified cybersecurity as an industry sector that is vital to Australia's long-term economic prosperity and national security.
- Australia spends approximately $3.2 billion on cybersecurity products and services each year.
- The majority of Australian organizations lack the capacity to employ large internal cybersecurity teams, creating demand for external, often international cyber services.
- 79% of their cyber expenditure is external, while only 21% is internal.
- The country's cyber sector is forecast to grow rapidly over the next 7 years to reach industry revenue of $4.2 billion and employ 31,600 people by 2026.
- The International Telecommunications Union's 2018 Global Cyber Security Index ranked Australia as the 3rd most committed country to cybersecurity in the Indo-Pacific region, and the 10th most committed country globally.
- Australia was ranked 2nd globally in the 2017 Global Open Data Index, which measures policies that support cybersecurity and allow government data to be openly available to the public.

CYBERSECURITY OVERVIEW

- The first national Cyber Security Strategy was released by the Australian Government in 2016. This strategy elevated cybersecurity to an issue of national importance and led to the establishment of AustCyber, the Australian Cyber Security Growth Network.
- The strategy, backed by $161 million of government funding, outlined 5 key themes and corresponding initiatives that the government intends to achieve by 2020.
  - National Cyber Partnership
  - Strong Cyber Defenses
  - Global Responsibility and Influence
  - Growth and Innovation
  - Cyber Smart Nation
- According to AustCyber, Australia must address the following major challenges:
  - Address the current skills shortage and workforce gap
  - Focus on research and development
  - Improve the incubation environment for startups
  - Enhance access to global markets
- AustCyber's research indicates that approximately 62% of Australian companies are looking to increase their overall security spending over the next 1 – 2 years.
- Demand for cyber services is predicted to experience 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.

CYBERSECURITY OVERVIEW

- 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 cybersecurity solutions to enable growth for a wide range of sectors:
  - Medical Technologies and Pharmaceuticals – improve healthcare networks and infrastructure; develop frameworks for improved clinical data sharing
  - Mining equipment, technology and services – improve the security across connected mining environments and the safe integration of legacy technologies and systems
  - Advanced manufacturing – improve channels for supply chain data sharing; ensure secure integration of cyber-physical manufacturing systems
  - Oil and gas – improve national and global intelligence sharing; implement active education programs
  - Food and agribusiness – improve collaborative data sharing; build awareness of cyber solutions

CYBERSECURITY GOVERNMENT FUNDING & INITIATIVES

- In the lead-up to the federal government election in May 2019, the Australian Liberal Party committed to providing $109 million to boost the Australian cybersecurity sector through several key initiatives:
  - Creation of a $35 million Cyber Security National Workforce Growth Program
  - $25 million to support the Australian Cyber Security Centre
  - The creation of cybersecurity 'SPRINT' teams
  - Development of a Cyber Security Response Fund
  - $28 million funding to assist the Australian Defense Force to grow its cyber warfare workforce, creating 230 new military cyber specialist positions
- In 2018, the AustCyber Projects fund provided $4.5 million funding across 10 projects. In 2019, an additional $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.
- Virginia companies can capitalize on the funding initiative by partnering with local Australian companies with complementary technology solutions or services.

CYBERSECURITY OPPORTUNITIES

Critical Infrastructure

- The government established the Critical Infrastructure Centre in January 2017.
- The Centre safeguards Australia across 8 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
  - 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 if critical infrastructure to undertake certain activities in order to mitigate against a national security risk.

CYBERSECURITY OPPORTUNITIES

Healthcare

- There are about 695 public hospitals and 630 private hospitals across Australia. As one of the most data rich sectors vulnerable to ransomware and other attacks, the sector faces the challenge of balancing security with accessibility to patient records and delivering a patient-centric approach to healthcare.
- 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 from October 1 – December 31, accounting for 54 of the 262 breach notifications received.
- In response to increasing cyber threats, the Australian Digital Health Agency (ADHA) established a dedicated Digital Health Cyber Security Centre in 2017.
- The Centre's goals to strengthen the security of Australia's digital health systems and services will be achieved through the following key initiatives:
  - Establishing partnerships with a range of national and international cybersecurity organizations in order to improve knowledge of cyber threats and leveraged shared experience and best practices
  - Development of cybersecurity guidance materials and threat intelligence
  - Undertaking operation security activities and incorporating security in the design of national digital health systems
  - Coordinating security incident response activities related to digital health systems
  - Developing a toolkit to assist healthcare businesses to select secure IT products and services

CYBERSECURITY OPPORTUNITIES

Defense

- Defense has one of the largest ICT networks, as it supports a wide range of military, administrative and management capabilities.
- Under the ICT Investment Plan, Defense is expected to spend $664 million in 2019-20.
- The Chief Information Officer Group (CIOG) within the DoD leads the integrated design, cost effective delivery, and sustained operation of Defense's Single Information Environment (SIE) to support military and business operations.
- In January 2018, the defense sector established 2 new cyber units to work alongside the Australian Signals Directorate (ASD): SIGINT (signals intelligence unit) and Cyber Command. These units stress the sector's growing focus on cyber security measures and proactively identifying and mitigating cyber risks.
- Virginia companies interested in working as contractors to the Australian DoD are encouraged to undertake the following steps:
  - Implementing and demonstrating compliance with the mandatory Strategies to Mitigate Cyber Security Incidents published by ASD.
  - If sub-contractors are engaged, contractors must ensure that they establish prescriptive cybersecurity requirements and retain some level of control over the supply chain by gathering evidence of compliance with the established terms.
  - Virginia companies should proactively provide information, undergo up-front risk assessments and obtain cybersecurity assurances in order to preemptively address any potential risks associated with contracting as an overseas supplier.

CYBERSECURITY OPPORTUNITIES

Banking, Financial Services & Insurance (BFSI)

- 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, ex: 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
  - 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 Virginia exporters. Examples of initiatives implemented by actors within Australia's BFSI sector over the past 12 months include:
  - The Reserve Bank of Australia has been prioritizing cybersecurity in the supervision of Australia's financial market infrastructures, also reviewing ASX companies against international cyber resilience guidelines
  - The Australian Securities and Investments Commission has been reviewing the cyber resilience of financial sector firms it regulates
  - SWIFT introduced a program to establish mandatory controls for security, guidelines for monitoring network breaches, and a protocol for sharing information on attacks

MARKET ENTRY STRATEGY

- Virginia companies interested in exploring opportunities in Australia's cybersecurity sector are encouraged to undertake the following key steps:
  - Understand the market and customer demand
    - Engage with industry associations for cybersecurity in Australia and subscribe to industry publications to stay up to date on current issues
    - Participate in a market visit in order to gather additional market intelligence and meet with prospective partners in person
  - Select the most suitable partner and/or establish a local presence
    - 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

Supplying to Public & Private Sectors

- The process of supplying cybersecurity services will differ if end customers are in the public sector (defense), private sector (BFSI), or a combination of both (healthcare).
- The Selling to Government guide published by the Department of Finance provides potential suppliers with relevant information related to the bidding process.
- Companies interested in supplying to the private sector are encouraged to conduct research and identify specific organizations demonstrating a commitment to invest in cybersecurity solutions/services, and may therefore represent potential end users.
  - Virginia companies should seek to identify and appoint a local partner that has established relationships with key stakeholders in 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.