BUILDING AUSTRALIA'S CYBER SECURITY INDUSTRY AND CAPABILITY

REPORT FROM THE ADC FORUM DIALOGUE
CYBER SECURITY – CHALLENGES AND OPPORTUNITIES
IN COLLABORATION WITH THE SOUTH AUSTRALIAN GOVERNMENT
HELD ON 2 SEPTEMBER 2020

On 2 September 2020, ADC Forum, in collaboration with the South Australian Government, hosted a dialogue on cyber security with leading Australian and international cyber security experts in a revealing open and online roundtable discussion which provided exceptional insights for business leaders and policy makers. The panel found the risks are real, but so is the opportunity, which is the opportunity to grow the cyber security ecosystem in Australia and create economic growth, stability and attractiveness to overseas investors. This report synthesises the expert discussion and proposes actionable insights for government and industry, on understanding the opportunity to build the cyber security industry as part of the cyber economy and how we as a nation grasp it.

Cyber security is one of the top risks to commercial activity. Businesses worldwide spend approximately USD$84 billion in defending data breaches that eventually end up costing them USD$2 trillion in damages. This could increase to USD$90 trillion by 2030 if cyber-attacks remain unchecked. Only this June, the Australian Prime Minister announced that Australian organisations were currently suffering a 'sophisticated' cyber-attack from another country, which he declined to name.

We live in an increasingly interconnected digital word. While this affords us convenience, speed and unprecedented access to information, it also exposes us to risk. Risk to government, essential infrastructure to corporations and to every one of us with digital connections and devices. In this new world, cyber breaches and attacks are an ever-present threat. They will happen, and we will not be able to predict them. We need to be able to constantly monitor, react to and mitigate these events before they cause systemic damage.

Emerging Outcomes

From this dialogue, the following recommendations and proposed actionable agendas have emerged:

1. **A focused dialogue**

ADC Forum **convene a cyber security council** to work with governments and industry to develop a comprehensive plan to grow the Australian cyber-economy.

2. **A growth agenda**

A pro growth agenda with actionable steps to accelerate growth in the cyber economy, facilitating cross-sectoral and interdisciplinary engagement, outreach and collaboration across the cyber security ecosystem. This agenda should create incentives to invest in building the Australian cyber industry, and give measurable growth targets for the cyber economy.

3. **A capability agenda**

A comprehensive cyber security capability agenda, with new thinking for developing talent and R&D capability, including leveraging our geographic position in Asia, enabling exchange, collaboration and incentives to attract talent.

4. **A public education agenda**

A comprehensive cyber security public education agenda, to make critical industries and their boards more aware about the cyber security risks and local capabilities to support them.

5. **A collaboration agenda**

The Government explores an ambitious collaboration agenda based on a cyber security – super cluster model. Super clusters are consortiums of businesses, research organisations, tertiary and vocational training schools, and nonprofits. These interest groups work together to develop digital talent, innovations and turn profitable and efficient technological centres that foster economic growth, employment and technological advancements.

State of Cyber in Australia

The need for companies to find new ways to enhance security has never been greater. Some recent statistics from the Australian Information Commissioner on Australian cyber attacks illustrate the magnitude and speed of the risk:

- $2.3 billion was stolen by cyber criminals from Australian consumers in 2017.
- 964 data breach notifications were made under the Notifiable Data Breaches scheme from April 2018 to March 2019, 60 percent of which were malicious or criminal attacks.
- 53,474 reports were received by the Australian Cybercrime Online Reporting Network in the 2017/18 financial year, and 64,528 in the 2018/19 financial year.

- 2500 percent increase in the sale of ransomware on dark net sites between 2016 and 2017, with basic tools costing as little as $1.30
- 250 percent increase in the share of inbound emails that were phishing messages in 2018 alone.
- $2.1 billion per year, at least, is the estimated economic impact of identity crime in Australia.
- 80 percent of victims receiving assistance from IDCare, Australia and New Zealand's national identity and cyber support service, reported a psychological impact.
- 34 perfect of breaches involve internal actors, including malicious attacks and negligent use of systems and data by employees.
- "Cloud jacking" of an organisation's cloud infrastructure is likely to emerge as one of the most prominent cybersecurity threats in 2020. 5G to Wi-Fi security vulnerabilities will be exposed in 2020. With 5G rolling out across expansive public areas, the voice and data information of users on their cellular-enabled devices gets communicated via Wi-Fi access points.
- Mobile devices can also conceal signs indicative of potential phishing attacks and other cybersecurity threats. Watch Guard predicts that 25 percent of data breaches will involve off-premises devices.

Last month the Australian Government released *Cyber Security Strategy 2020* which will invest $1.67 billion over 10 years. The themes are very much of a risk mitigation focus, protecting and defending critical infrastructure, shutting down cybercrime, improving the defence of Government networks and data and guidance, education and community awareness and collaboration to build Australia's cyber skills pipeline. The vision however, is pedestrian: "A more secure online world for Australians, their businesses and the essential services upon which we all depend". Contributors to the dialogue challenge the government to lift its gaze, stop playing a defensive game and embrace the opportunity to grow a cybereconomy in Australia. There is no reason Australia cannot be a world leader in cyber innovation, driving economic growth and delivering benefits to Australians and our region.

Cyber-business opportunities for Australia

Global demand for cyber security is surging. The global value of cyber security was USD$131b in 2017 and is set to reach a value of USD$270b by 2026. Australia is the second most developed nation in the Indo-Pacific region in terms of cyber maturity and our strength in core areas of computing presents a valuable growth environment for cyber security firms.

The Australian Cyber Security Growth Network (ACSGN) report cyber security is a growing sector in Australia, but not in a purposeful, focused manner. It currently employs around 20,500 people with total expenditure of A$5.0 billion in 2018. More than three-quarters of the market is dominated by foreign companies, mostly with local bases employing Australians. According to contributors to the dialogue and data from ACSGN, there are no local companies among the 15 largest software providers by value in the Australian cyber security market and the market share of Australian companies is estimated to be less than 5%. There are no major Australian hardware providers. It is estimated that the share of Australian services companies is about 25% with 50% served by foreign-owned companies with core personnel in Australia.

'Business-as-usual' forecasts suggest revenues in the Australian cyber security sector could more than double from A$2.2 billion in 2016 to $4.7 billion in 2026. AustCyber report that Australia can compete in software (in areas of distinctive research capability) and services (in the protection stack and underlying processes). In this case, revenues in the domestic cyber security sector could increase to A$6.0 billion in 2026, which equates to an annual growth rate of almost 11 percent over the decade. If Australia could match the performance of global leaders such as the US and Israel, the cyber workforce would expand to almost 60,000 jobs with industry revenue of $11 billion in 2026.

Furthermore, strong cyber security will enhance Australia's global reputation as a trusted and secure place to do business and will be the foundation for future success of all industries in the national economy. Yet few senior executives see cyber as a road to growth. A 2016 Cisco survey of senior executives across 10 countries including Australia, found that only one-third believed the primary purpose of cyber security is to enable growth. Most still see it as risk reduction and threat protection.

When compared with the rest of the world using a revealed comparative advantage measure, Australia significantly under achieves in areas of software and hardware development while overperforming in services. Again, comparing Australia to the rest of the world, we significantly outspend other nations in the cyber security coverage of financial services, government departments and telecommunications, while significantly underspending in retail, construction, utilities, and other key areas of industry. The difference between strong cyber leading to a positive future, and weak cyber leading to a lack of trust and investment, could be more than 1 percent higher GDP by 2026.

Australia has not created the ecosystem for Australian firms to thrive and grow and several notable cyber security companies (such as DTEX and Quantum Laboratories) have had to leave Australia for investment and have proven their success, even in highly competitive markets such as the US and Europe. Much has been achieved since the Sector Competitiveness Plan was first published in 2017, but more action is needed to grow a vibrant and competitive cyber security sector that generates increased investment and jobs and there is an urgent need to address skills and workforce shortage.

Building Australia's Cyber Economy

Building Australia's cyber economy will require a purposeful focus on four actionable agendas:

1. A growth agenda
2. A capability agenda
3. A public education agenda
4. A collaboration agenda

1. Growth Agenda

Australia has much to learn from other countries, who have been purposeful in building the cyber economy. Israel, a country one third of Australia's population is considered a leading cyber nation. The government is leading in the coordination of the development of a system to deal with unpredicted cyber threats, and putting resources into cybersecurity education which begins as soon as middle school. Teaching cyber security and coding in its public schools generates the future digital workforce, many of whom continue in army cyber security units and go into the private sector to found or work for start-ups. The Israeli government also incentivises and makes resources available to help those companies market themselves around the world. Available data indicates Israel has around 200 to 250 cyber workers per 100,000 people. In Australia that number is around 80. There is much to be done.

Building the cyber ecosystem will be a collaboration among entrepreneurs, academics, government, industry and private capital. Purposeful building will require fostering those partnerships that will develop, and scale the cyber innovations that will grow our economy. This should be in the areas identified as Australia's competitive advantage in software (in areas of distinctive research capability) and services (in the protection stack and underlying processes).

The Asia-Pacific region is rapidly emerging as a key cyber security market. Australia's location in this region is an advantage. Southeast Asian organisations are investing heavily in cyber security services and solutions, with spending rising by an average 15% per year. Austrade and AustCyber estimate a potential market opportunity worth A$7.3 billion for Australian cyber security businesses.

The policy and regulatory environment is a critical facilitator of cyber security innovation. This will require strong incentives for elevating the cybersecurity innovation agenda at the national, provincial, and municipal levels, supported by a thriving cybersecurity innovation ecosystem fosters a highly skilled talent pool, a cyber-aware population, and first-mover access to the latest cybersecurity products and services to secure government and private sector systems. Specific actions for consideration could incorporate:

1. De-risking innovation and helping firms of all sizes to go beyond their existing capabilities and what they can achieve with their own resources;
2. Developing a pipeline of opportunities through defined programs and co-investing with quality consortia;
3. Set benchmarks for government and industry to spend a percentage of budgets with Australian cyber security start-ups and companies (startups to be vetted by AustCyber);
4. Build private risk capital, angels, super angels, corporate venture capital, family offices - incentivise the local investors to invest in Australian companies, including investment into augmenting and improving established businesses to move laterally into cyber and grow adjacent industries; and
5. Use the legal and regulatory framework to incentivise ecosystem.

2. Capability Agenda

Countries that lead the world in innovation have learned to build talent, large scale R&D that harnesses the strength of their innovation ecosystem.

2.1 Talent

In 2017, AustCyber reported that Australia's cyber security workforce was 19,500. 9,000 in internal security operations for Australian organisations, 11,000 in the external security services industry and only a minority working in cyber security hardware and software development. This included growth over the previous two years of 7% - roughly 3.5% per year. It probably needs to be of the order of 10% per year for a full ten years if the gap identified is to be met. More pathways are needed for workers to transition from the broader IT sector and other industries. The deficit of skills is likely to become a growing matter of public concern during the early part of this new decade.

Australia's economy is more and more relying upon software and software builders. Local tech-unicorns like Atlassian, Canva, WiseTech are changing the world, and more of our critical industries (banking, government, mining) are exponentially hiring software engineers and developers.

The education system is mobilising but will fall short. Universities and TAFEs face a shortage of teachers, a lack of adequate funding for technical infrastructure and low student demand. Approximately half of Australian universities now offer cybersecurity as a degree or a major for IT courses. There is a lack of university degree programs or professional education in advanced cyber operations and a weakly developed national capability for complex cyber exercises.

There is a risk that we are producing insecure software and software engineers who have no proper "safety" training. Our banks will become vulnerable to attacks, our mining industry will as well and our tech-giants will have their IP stolen. Similarly, many hundreds of IoT devices that are misconfigured or insecure that every Australian will deploy in their homes in the next few years. If you look back to the data breaches in Australia, most of them can be traced back to a software or configuration error by a human. In order to stop this, we need to make sure our students are not only trained in building code, but in building secure code. Such certification needs to exist for anyone who is building code that will run in our homes, government and industry.

Australia should also explore new thinking for developing talent, like a national cyber war college, and a cyber civil reserve force, to drive our human capital development.

Not all talent can be home grown, the Australian Government’s Global Talent Visa program, launched in June, is a streamlined visa pathway for highly skilled professionals to work and live permanently in Australia. Cyber security is one of the skills areas, so targeting key global talent to come to Australia under this program is an essential part of talent development.

2.2 Research and Development (R&D)

There is also a lack of coordinated focus in research and commercialisation and scattered public funding weakens Australia’s ability to lead on cyber security. Australia should concentrate R&D on areas of strength and sector segments of software, security operations, and underlying processes. We need to leverage the capability in the research sector and create strong collaborations between research and industry and incentivise local R&D, and to translate scientific discoveries into products and services that can be used domestically and exported. R&D should also support research into new threats (and solutions) due to complex emerging technologies, especially the intersection of AI and Cyber (echoing the emerging tech research lab recommendation from Australia's new Cyber Security Strategy).

Australia should capitalise on location in Asia and invest in collaborative R&D with leading Asian Technology Institutes and create visa programs to attract R&D talent to Australia.

Specific actions for consideration could incorporate:

1. Further research to understand the impact of cyber security on the growth outlook of the Australian economy could help to change this mindset and support appropriate investments in cyber capability by Australian organisations;
2. For enabling industry, extend the cybersecurity concept into digital trust and trust-by-design (security/privacy/compliance-by-design), and use trust as the added value to traditional industries (such as manufacturing industry's increasing IoT/SaaS-enabled

manufacturing products), echoing Andrew Steven's recent piece on post COVID19 manufacturing industry's competitive advantage being in "confidence, trust and privacy" in products;

3. For capability and SME, build scalable cyber workforce capabilities by human and machine working together better. Promote machine-understandable cybersecurity standards and automated compliance (rather than relying on compliance officers alone);
4. A cyber security education fund with an initial investment of around A$1 billion to support a new national cyber college. It should be networked around the entire country, and independent of control by any existing education institutions, drawing on their expertise and that of the private sector.

3. Public Education Agenda

It is essential to create cyber security awareness. Corporate executives, SME's and the general public have to be on the frontlines of the cyber security agenda, for industry and Australia's national reputation as a safe place to do business.

Specific actions for consideration could incorporate:

1. Thought leadership series with education of executives is very important;
2. Creating requirements for listed companies to manage cyber risk and have a chief cyber officer;
3. Fund cyber startups to work on developing accessible cyber tools for SMEs; and
4. Implement a national campaign to understand problem with training and broader awareness for mass consumption.

Convergence – the Australian Cyber Supercluster

"Innovation Superclusters" of organisations across sectors and innovation ecosystems have stronger connections, a long term competitive research and innovation advantage, global brand recognition and outsized positive impacts on job creation and economic growth. These Superclusters are increasingly being seen as future engines of economic growth. They are built around industries of the future and can accelerate transformation and drive system level infrastructure at scale. An innovation Supercluster needs to be ambitious, bold and enterprising.

Australia should follow the lead of Canada and adopt a digital-supercluster development scheme. Superclusters are consortiums of businesses of various sizes, research organisations, tertiary and vocational training schools, and nonprofits. These various interest groups work together to develop digital talent and innovations within a local geography and in turn produce profitable and efficient technological centres that foster economic growth and digital advancements. Canada's supercluster was seeded with $360m which is expected to produce $5b and over 13,000 jobs in the next decade. A similar approach in Australia will ensure that our next generation of digital leaders will have an institutionally backed cyber security awareness.
It would require a coalition of government, corporates, academia, entrepreneurs and capital and would build a system level innovation engine for industries of the future. "Hyper-collaboration" based on innovation ecosystems, not individual companies, will be key. Innovation ecosystems bring together diverse and complementary capabilities from across the globe. These will be new collaborations for ecosystems that don't normally collaborate or converge.

ACKNOWLEDGEMENTS

We are very grateful for the insights provided through this dialogue by government leaders and international and Australian industry experts in the discussion
Cyber Security – Challenges and Opportunities on 2 September 2020.

Discussion Leaders:

The Hon Steven Marshall – Premier, South Australia
Anton Roux – CEO, ADC Forum

Contributors:

Andreas Baumhof – Vice President Quantum Technologies, QuintessenceLabs
Pieter Danhieux – Co-Founder, Chair/CEO, Secure Code Warrior
Stuart Davis – Global Head, Financial Crimes Risk Management, Scotiabank
Nik Devidas – Managing Director, Rock IT
Matt Faubel – Chair, Program Committee, ADC Forum
Bello Hayatudeen – Head, Virtual Assets & Cyber Intelligence, Financial Intelligence Unit, Nigeria
Loretta Joseph – Fintech and regulatory senior consultant, Financial Services Commission Mauritius
Mohan Koo – Co-Founder and CTO, DTEX Systems
Alastair MacGibbon – Chief Security Officer, CyberCX
Adrian Turner – CEO & Director, Borondi Group
Liming Zhu – Research Director, Data61, CSIRO

Report prepared by:

Dr Jane Thomason – Member, ADC Cyber Security Council

NOTE

The aim of the webinar and this report is to present current information and insights and expose arguments relevant to understanding this significant topic.

ADC Forum does not necessarily endorse any of the viewpoints, but presents them as a contribution to informed discourse and decision making on issues critical to our future.