KPMG

# Cyber Security

## Designing a Government-Business Partnership in Australia

# Foreword

Cyber security is vital to the long-term integrity of KPMG and our clients – as it should be for all organisations.

Cyber security can help differentiate a business from its competitors – for both good and concerning reasons. Cyber security is also one of the most exciting and innovative industries, and it is unlocking business and employment opportunities across all sectors.

KPMG has invested heavily in its global cyber security business, developing unique capabilities and establishing Centres of Excellence in Europe and the Asia-Pacific. KPMG monitors global trends and the approaches different governments take to confronting the opportunities and risks associated with cyber security. The lessons learned suggest governments with a proactive and progressive approach to cyber security can have a disproportionately positive impact on their businesses, economy and national resilience. A common feature of the most effective national approaches to cyber security is a robust relationship between governments and business.

In mid-2015, KPMG participated in the first Cyber Security Summit led by an Australian Prime Minister. The Summit brought together political and business leaders from across the economy to consider how Australia should confront the security, technical and economic challenges of cyber security.

KPMG also sponsored the inaugural Australian Security Summit, where the government-business interface of cyber security was a major theme. Such events recognise the necessity of active government and business involvement in positioning Australia to take full advantage of the digital age. This will require an ongoing, national conversation that permeates all businesses and governments, coupled with investment and action.

The release of this discussion paper, Designing a Government-Business Partnership in Australia, has been released as a thought-provoking stepping stone between the 2016 Defence White Paper, in which cyber features prominently, and the Government's much anticipated Cyber Security Strategy. We hope it makes a valuable contribution to this rare national conversation that traverses national security, our economy and society.


**Steve Clark**
**National Sector Leader, Defence & National Security**
+61 3 9288 6937
steveclark@kpmg.com.au

**Anthony Court**
**Lead Partner, National Security**
+61 2 6248 1102
acourt@kpmg.com.au

**Mark Tims**
**Partner, Technology Risk**
+61 2 9335 7619
mtims@kpmg.com.au

**Gordon Archibald**
**Partner, Cyber**
+61 2 9346 5530
garchibald@kpmg.com.au

# Cyber security – an issue too big to ignore

## THE CHALLENGE FOR EXECUTIVE ATTENTION

The imperative for initiating and maintaining cyber security vigilance is not immediately clear. Making the business case for senior leaders is challenging for a number of reasons.

Unlike public safety issues, it takes imagination to understand the risk to human life of malicious cyber activity.

Unlike terrorism, cyber security rarely occupies the front page of newspapers or becomes an electoral issue.

Unlike physical theft, the risks of cyber security are intangible and difficult to conceptualise.

Unlike environmental protections, there is no well-tested legal and regulatory framework for cyber breaches.

Unlike a major fall in a share price, there are few examples of executives being held accountable for failing to protect company brands and bottom lines from cyber attack.

**1131** cyber incidents responded to by the Australian Signals Directorate in 2014 [1]

**21.5 million** the number of people impacted by the US Government's Office of Personnel Management breach [2]

**8.5 billion** estimated value of Israel's cyber security industry in 2014 [3]

**565 billion** estimated annual cost of cyber attacks to businesses globally [4]

**35%** of Australian CEOs believe they are 'fully prepared' for a cyber-security event [5]

**25%** of Australian CEOs think cyber security is having the biggest impact on their company [6]

**29%** of Australian CEOs cite information security as the risk they are most concerned about [7]

[1] ACSC Threat Report, 2015.

[2] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[3] Reports of Israel's National Cyber Bureau figures.

[4] Lloyd's of London Chief Executive Officer, Inga Beale.

[5, 6, 7] http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/global-ceo-outlook/Pages/cyber-security-insights-2015.aspx

The numbers are concerning, but many governments and businesses are yet to move cyber security consciously and permanently into the boardroom.

In Australia, political and executive-level commitment to comprehensively address cyber security is sporadic. Executive attention peaks after something goes wrong, or when the time between reviews and investments has become obvious. Most governments and businesses appear to be struggling to position cyber security within the organisation as an enduring risk and genuine opportunity for innovation. The reasons are many, with some listed in the adjacent box. Thankfully, KPMG's work with businesses and governments, at all levels, would suggest this is slowly shifting.

But as events such as the US Office of Personnel Management breach and Israel's growing share of the global cyber security market demonstrate, this is not an area that rewards retrospection or incrementalism. Rather, success is achieved by integrating cyber security into the fabric of government, business and society. KPMG believes the key ingredient for such integration on a national level is proactive and sustainable collaboration between governments and businesses. Internationally, governments and businesses have been talking to come to grips with technology-enabled risks, with some genuine progress made. In Australia, successive governments have laid the foundations for government-business cooperation on cyber security. However, deliberations at the inaugural KPMG sponsored Australian Security Summit revealed more needs to be done to entrench a genuine partnership.

The Australian Government's Cyber Security Review, currently being considered by the Government, represents a major opportunity to implement bold, practical initiatives that could make Australia a global leader on cyber security. This paper explores the need for government-business partnership on cyber security, the features of a genuine partnership and priorities for action.

## An Australian cyber partnership – on the cusp

Australia is on the precipice of genuine collaboration on cyber security. Political and business leaders from outside the technology and security sectors are recognising the importance and opportunity associated with cyber security.

The Turnbull Government's new National Innovation and Science Agenda pledged to provide A$30 million through to 2019-20, to help create opportunities for businesses in the cyber security sector. The Government also announced the establishment of a new industry-led Cyber Security Growth Centre to help strengthen the industry.[8]

The global cyber security market is currently worth more than A100 billion and is growing at around eight percent a year. A Cyber Security Growth Centre will ensure that Australia is a global industry leader, able to export products and services in the global marketplace while helping Australian businesses and governments to address the growing threat of cyber crime.

The Cyber Security Summit hosted by the then Australian Prime Minister, the Hon Tony Abbott MP, and involving CEOs from leading businesses, including KPMG's CEO Gary Wingrove, is a clear indicator the Australian Government has acknowledged the criticality of government-business cooperation on cyber security. Policy continuity is anticipated under the Turnbull Government. Given Malcolm Turnbull's background and policy directions contained within his Innovation Statement and the 2016 Defence White paper.

Business is also backing opportunities for collaboration and information sharing. KPMG sponsored the inaugural Australian Security Summit, which was attended by senior members of Australia's intelligence and policy community, academics and think tank representatives and leading business figures. All participants, including intelligence officials, engaged openly in this 'unclassified' forum.

Despite these positive signs, few governments have successfully evolved policy statements, one-off events or transactional information sharing activities, into dynamic, collaborative partnerships. Participants at the Australian Security Summit explored why. Answers ranged from cultural impediments, commercial risks and a lack of resourcing, through to difficulties in making a compelling business case for resources in a fiscally constrained and highly-competitive environment. Many of these are legitimate justifications. None are insurmountable.

Leadership and commitment from government, coupled with investment and support from the private sector can help dissolve these barriers. Some countries have taken steps to entrench the relationship in a formal partnership. The inaugural BSA APAC Cybersecurity Dashboard found a few leading countries have established formal public-private partnerships (PPP) in cybersecurity.[9] Australia, while advanced in other metrics, lagged. Indeed the recent announcement by the Government to deepen cooperation at an international level through the Australia-United States Cyber Security Dialogue is a welcome move to increase the knowledge sharing of risks and opportunities.[10]

While it is unclear if there is a need for a formal PPP, there are benefits in establishing a framework to drive outcome-focused cooperation. Or, put more simply, a national partnership. While the digital economy and cyber threat landscape is global, interlocking government and business efforts on cyber security can deliver national benefits.

[8] http://www.innovation.gov.au/page/cyber-security-growth-centre

[9] http://cybersecurity.bsa.org/2015/apac/assets/PDFs/study_apac_cybersecurity_en.pdf

[10] https://www.pm.gov.au/media/2016-01-20/australia-and-united-states-strengthen-ties-cyber-security

## Cyber security – a challenge for both government and business

For those directly involved in cyber security, including some political and business leaders, there is a belief that the case for a national cyber partnership is self-evident. Neither side exclusively possesses the factors needed for a robust and sustainable approach. However, unlike most emerging challenges, the core dimensions of cyber security are shared by governments and business.

- **It is a major risk for both.** Malicious cyber actors are targeting governments and businesses for a variety of commercial, financial, strategic and political objectives. Cyber attacks can undermine public confidence, erode the bottom line, limit support for new initiatives, give competitors a strategic edge and irreparably damage brands or personal reputations.
- **It is an opportunity for both.** An effective cyber security posture can attract business, enable market differentiation, increase consumer confidence and adopt more cost-effective practices. Cyber security is also a growth industry, with potential for high-cost, knowledge-driven economies such as Australia.
- **Vulnerabilities for one creates risks for others.** The internet of things and globalisation have created multilayered, global connectivity. Businesses and governments do not exist in isolation. A company's failure to have a mature approach to cyber security can have significant flow-on effects to a nation's citizens and economy. Equally, slow-moving or risk averse government practices can increase the risk exposure of businesses of all sizes and natures, and disadvantage businesses relative to international competitors.
- **Both compete for the same staff and services.** The features of an effective cyber security posture do not differ greatly between the public and private sector. While creating a front for collaboration, it also amplifies the pressure on the cyber security jobs and services market. There is a dearth of competent cyber security professionals. There is scarcer availability of professionals with a balance of tech expertise and business acumen.
- **Maintaining focus is a challenge for both.** The business case for ongoing cyber vigilance is not easily made in most public or private sector organisations. Currently, electoral or investor pressure is generally only retrospective. Justifying appropriate and ongoing investment is difficult for public and private sector organisations, absent of a quantifiable risk picture, which differs for each company and government.
- **Neither side can see all the data.** Private sector and not-for-profit organisations are gaining a greater picture of the cyber risk environment. However, law enforcement and national security intelligence agencies see some unique and different data. Governments can work across all sectors of the economy and with other national governments to detect and analyse emerging trends. Only by working together can a complete picture be established, which will enable swifter and more resilient responses.

## There are some areas where governments and businesses have a relative advantage

- **Governments set the rules, mostly.** Regulations and laws, set domestically and internationally, are likely to have an increasing impact on business behaviour and the development of the cyber security sector. Responding to electoral, business and national security pressures, governments are more actively exploring options to optimise the cyber security regulatory framework. Companies will exert increasing influence via lobbying and multi-stakeholder forums. But creating and removing laws and regulations remain the remit of governments.
- **Business has greater capability and drives innovation.** Just as the private sector has driven the creation of the internet of things, so too will it provide the necessary technical solutions for citizens, businesses and governments. The private sector can respond to changes and new threats more quickly than governments. The private sector is the key driver for the development of a larger and more skilled labour pool.
- **Governments are, on the whole, more trusted.** This view may not be shared by certain quarters of society and some businesses may be reluctant to share information for fear of investigation or regulation. However, governments can act as honest brokers, particularly at this relatively early stage of Australia's cyber security journey. International experience suggests this role is vital for cross-sector collaboration arrangements.

As was evident at the Australian Security Summit, there is common ground for government and business consultations. Governments and businesses should collaborate on shared challenges by playing to their respective strengths.

## Principles for partnership

Public-private partnerships (PPPs) work well domestically and internationally. Infrastructure offers possibly the most mature field of PPPs, and there has been much academic research into the features of effective PPPs. Guiding principles can help with the transition from relationship to partnership.

These are guiding principles or key features of a successful partnership only, and could be developed into a set of detailed and fit-for-purpose operating procedures or charter. However they offer a starting point on which a partnership model could be established.

| | | |
|---|---|---|
| 1 | Focus on respective strengths | Governments should not do the things the private sector can do better, and likewise in reverse. This can help determine whether the relevant public or private sector organisation should take the lead for specific initiatives. |
| 2 | Agree clear priorities for shared action | Good strategy should be followed by clear identification of supporting activities and the resources available to achieve the objective. Establishing this shared mission and mutually-agreed priorities will ensure focus. Setting priorities to include some 'early wins' will help with proof of concept and to gain momentum for more challenging priorities. |
| 3 | Be ambitious but practical | Modest goals are unlikely to inspire the imagination or offer sufficient return on investment for political or business leaders. Equally, goals that are intangible create a perception of another government-business 'talkfest'. Clear actions that deliver practical returns will help make the business case for taking risks and providing resources. |
| 4 | Identify clear leadership roles and accountabilities | Effective partnerships need clear and consistent leadership, whether it be an organisation (government department or business), individual (senior executive or minister) or a small group.[11] In a government-business partnership, leaders are required to drive outcomes, identify and overcome barriers to progress, and communicate with identified stakeholders. Leaders need to be clear on what they are expected to deliver, timeframes and agreed standards. |
| 5 | Actively measure and report progress | There is often reluctance to measure progress in the public sector. It is hard and certainly not a pure science in a public setting where political imperatives can be at play. However, the process can help to build trust among stakeholders. It is also likely to improve the overall efficacy of the initiative as it allows the identification and application of resources to more successful or more challenging initiatives. |
| 6 | Be inclusive but selective | Governments need to be open in establishing partnerships. Initiatives will benefit from diverse views and contestability. It is also important to minimise the perception of picking winners. There are risks from some private sector participants pursuing short-term commercial objectives ahead of the shared mission. Accountability and manageability should not be compromised for the sake of maximum inclusivity. |

[11] http://www.uli.org/wp-content/uploads/2005/01/TP_Partnerships.pdf

# Designing an Australian cyber partnership

The momentum built by the Government's Cyber Security Review, is an opportunity to seize. Government and business leaders should move to formalise the government-business groupings formed to support the Review into an outcomes-focused partnership. This will require leadership from government and genuine commitment from business. It will also require the design of a sustainable business model with effective governance and a clear idea of immediate priorities for the partnership.

This section sets out a possible governance structure and identifies a few areas ripe for the partnership's immediate focus.

## A viable (initial) business model

Figure 1 below sets out a high-level governance structure for the partnership.

This structure allows for: strong government oversight; clear accountability; and joint government-business involvement in all aspects of the programme. Possible roles and responsibilities of the various components are detailed in the table below. However, consideration also needs to be given to the overall role of government in such a partnership and how it might be funded.

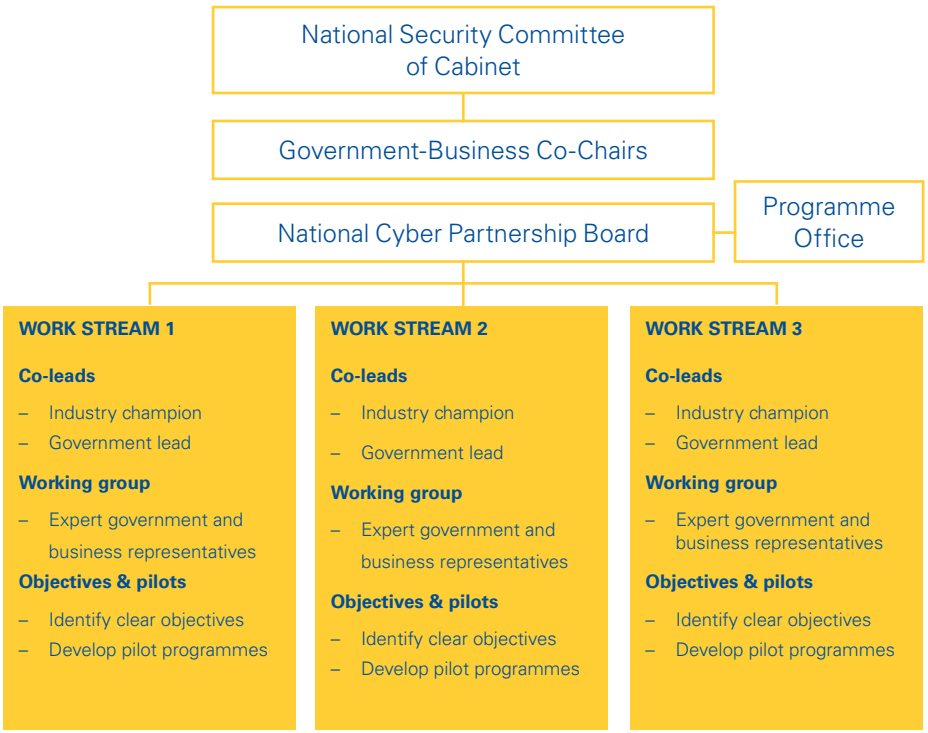


**Figure 1: National Cyber Partnership Governance structure**

Just as a company's business model might evolve as it matures, so too can we expect the roles played by Government and business to evolve. Initially, Government, up-to and including the Prime Minister, will need to play an active role in the partnership. For while there may be some areas or specific activities where the weight of effort will be by industry figures, providing leadership and acting as the honest broker will be important for the legitimacy of the initiative. Government support will also be required to overcome barriers and navigate the sensitivities inherent in a multi firm venture. Put in economic terms, Australian government intervention now can be argued on the grounds of correcting a market failure. The Government needs to ignite action with a strong upfront investment.

However, once the correction is made, government could taper its role, focusing instead on its core responsibilities, such as national security. This approach would be consistent with that taken by the Cameron Government in the UK.

As was also the case in the UK, the Australian Government will need to contribute resources and seed funding to kick-start the partnership. Government is likely to be required to be the lead funder of the Programme Office or secretariat, reflecting its strong interest in ensuring the functionality of the overall partnership. This should be complemented, on almost equal terms, by private sector contributions focused on specific initiatives. These contributions could include cash funding for specific initiatives, in-kind support, pro bono services and the provision of fully-funded secondees. Seeking, accepting and then allocating resources will be a major risk area, worn mostly by government, and vital to ensuring strong business buy-in. A trusted board, clear decisions and transparent process will be important ingredients.

## PROGRAMME OFFICE

Programme offices are used to varying degrees of success across government and the private sector. They can vary in shape, size and purpose depending on the nature of the programme.

To drive the implementation of a national cyber agenda, the Programme Office will need to be a standard bearer of action and innovation. It should integrate private sector representatives and be given a degree of autonomy from the established departments. Working across agencies with cyber responsibilities will be important if progress is to be achieved and vested interests wrested. While a challenge to these departments, creating an empowered Programme Office will address long-held industry calls for greater clarity in the Canberra bureaucracy and aid with accountability. The recently established Digital Transformation Office, which sits within the Prime Minister's portfolio, is a viable model on which to build.

## National Partnership – roles and responsibilities

### National Security Committee of Cabinet

The work conducted under the auspices of a government-business partnership should be accountable to the people of Australia through the Government. The National Security Committee of Cabinet (NSC) is the primary government decision making body on domestic and international security matters. While an argument could be made the economic aspects of cyber security necessitates the involvement of full Cabinet, the strong security-economic nexus makes the NSC the best home for consideration of cyber security. Other ministers such as the Minister for Communications should be involved.

### Government-business co-chairs

The Prime Minister should appoint a representative from government and business as the inaugural co-chairs of, or joint leads for, the partnership. This pair would chair the board proposed below and be responsible for reporting progress to the NSC.

The government representative could be part of the ministry or a senior official with the requisite authority. The business representative should possess strong business and leadership credentials who can work across multiple sectors. This person could be from the business side of the technology or telecommunications sector, and not a Chief Information Security Officer.

### Programme Office

The co-chairs and the board will need support to execute the Government's vision. A small organisation comprising representatives from government and business could be established as the policy and programme management engine room for the partnership. It will require a mix of cyber experts, experienced government officials and individuals with business acumen credentials to engage the various stakeholders. It should track progress, produce reports to aid transparency and engagement, and provide communications support. This may require a heavier up-front investment from government and could be spun-off once mature.

### National Cyber Partnership Board

The board should ensure the partnership is fulfilling the mandate as issued by the Government and provide the Government advice on future challenges and opportunities for Australia. The board would be responsible for guiding the development of a clear vision for the work. The board needs to be representative of the broader economy and could include representatives from not only business and the Federal Government, but also state/territory governments, academia or the think tank community. However, at this early stage, the board should not be too large, with members appointed by the Prime Minister on the advice of the co-chairs.

### Work Streams

To give the partnership life, a small number of work streams should be established to progress actions in the areas of greatest national importance. Each stream should have a clear industry and government lead, who can be accountable to the board for the work. This pair would be supported by a larger number of working group members – experts sourced from interested businesses, who would contribute funding, resources and time. Together they can develop clear deliverables, a detailed project plan and identify resource requirements for board-agreement. The size and nature of these working groups may evolve over time or could be dissolved once key objectives have been achieved.

## Priority focus areas

As the submissions to the Cyber Security Review reveal, there are numerous areas requiring action from the public and private sector. Many of the areas are not new and some will take longer to resolve than others. Three areas that could be game changers for cyber security in Australia include: government-business information sharing; developing a culture of cyber security; and Australia's domestic cyber security industry.

This section explores these areas and contributes practical suggestions that could be taken forward by the partnership.

## Improving information gathering and sharing

Australia needs more businesses actively sharing information on cyber threats and successful attacks. Government needs to get better at sharing high-quality and actionable information in a timely fashion.

Creating a culture of information sharing with trusted parties is the objective likely to make the greatest difference in Australia. It is only when vulnerabilities are exposed domestically that national defences and resilience can be strengthened. The Economist recently argued that creating a culture of openness is the best defence from malicious cyber activities for the very practical reason that it helps spread fixes.[12]

This issue was the most widely discussed in the cyber security sessions of the Australian Security Summit. Achieving substantive improvements is not without hurdles. Risks, perceived and actual, for government and business alike has created a clear gap in open cyber information sharing, in which only a fragmented bridge exists. On the government side, participants at the Summit heard of ongoing challenges of security classifications. One senior government official recognised that while considerable progress had been achieved in recent years, Australian intelligence and security agencies were yet to overcome a cultural resistance to pushing information to the lowest possible classification levels. On the business side, there were countless anecdotes of businesses not reporting or sharing information for fear of damage to brand equity, regulatory and legal recrimination, and providing competitors commercial advantages.

Around the world, various government-business information sharing models have been implemented, often to great success. One common feature in the more successful models is that government and businesses are more likely to share information where personal trust exists. This is not obviously practical on a large-scale information sharing program. But Australia can start to breakdown cultural barriers by ensuring human interaction between senior government and business leaders, and not just with CIOs and CISOs.

### MANAGING INFORMATION TO GAIN TRUST

Complete openness is still an aspirational target, particularly from a business to government perspective, where industry competitors will co-exist and a competitive advantage could be achieved. An appropriate information management system must exist to sanitise originator information, control access privileges, and define scope for dissemination. An often used model of information management within sharing forums is the Traffic Light Protocol (TLP). The TLP uses:

**Red:** Restricted within the Information sharing forum, restricted distribution list.

**Amber:** Restricted distribution list, can be disseminated externally to select parties .

**Green:** Free to share within the forum, can be disseminated externally to select parties.

**White:** Free for public sharing (within copyright and legal restrictions).

[12] 18 July 2015, The Economist, 'Embedded Computers: Hacking the planet'.

**Proposal 1: ACSC provides government liaison officers to establish the information sharing link between businesses (assigned and designated by sectors) and the ACSC and CERT.** The liaison officers are responsible for collection and dissemination of relevant cyber threat information, and sanitisation of the information for any wider dissemination beyond the ACSC. Such a model would clarify for business the single government point of contact. It could help focus resources in the highest priority sectors or areas, such as banking, mining and critical infrastructure.

**Proposal 2: Establish a centrally-located facility dedicated to the sharing of cyber threat information,** with graduated levels of security as a signal of openness and collaboration. This facility should be closely associated with, or an extension of, the ACSC, but not located in one of its member agencies. A baseline level of trust for interacting in such a facility can be established by government facilitating access to security clearances or non-disclosure agreements for access to lower-classification material. In return, all participating organisations would need to contribute information of a certain standard. State governments could be contributing members. Such a facility would be a powerful hub for improved reporting and protection and a powerful driver of cultural change in government and business.

**Proposal 3: Agree annual targets for the amount of timely information provided back to business** and targets for new businesses sharing information with the government. The vision of the ACSC has yet to be fully realised and in-part made harder by its physical location. There is also limited external attention paid to ensuring the ACSC and its member agencies are fulfilling this aspect of its mandate. The targets should contemplate exchange frequency but also value to the sector. Transparent reporting will help ensure appropriate focus is paid internally and externally.

## Create a culture of cyber awareness

There is a need to improve Australia's national cyber awareness. A Harvard Business Review article examining the US Department of Defense's improved approach to cyber security noted, 'in nearly all penetrations on the .mil network, people have been the weak link'.[13] Improved awareness should be achieved without a retrospective catastrophic cyber event, such as that experienced by one of the most digitally connected nations in the world, Estonia. Large-scale awareness campaigns such as those used for public safety issues like smoking, drink driving or wearing seatbelts are expensive and can take decades. That is not to say there is not a place for large national campaigns, with National Cyber Security Awareness Week providing an important focal point for the broad stakeholder group. However, for cyber security, where many of the same behaviours are relevant for the workplace or at home, there may be more effective approaches to achieving a national uptick in awareness.

Looking at this objective as a change management challenge provides an alternative prism to consider practical levers available in Australia. Overlaying the practices representing 'good' cyber security points to exciting interlocking initiatives that could be pursued as a package. Efforts should be prioritised toward raising the awareness of the largest employers in the public and private sectors.

The rationale for this focus is built on numbers: these organisations are likely to carry the greatest national risk; larger organisations will be more able to demand better cyber security practices from their extended supply chain; and, improved organisational cyber security is likely to result in an uptick in improved employee cyber security practices, which should have a flow-on for the broader Australian economy and society. However, the first challenge may be convincing public and private sectors leaders of the need to integrate cyber security into their organisations rather than it being a retrospective add on or compliance exercise – making this ripe for the concerted effort of a national partnership.

There is no one-size-fits-all approach to achieving cultural change, but a common feature is leadership understanding of the need for change and taking ownership of the new vision. There needs to be alignment between strategy and organisational culture to drive change. Despite some Australian public and private sector leaders now integrating cyber security into the operation of their organisations, there is far from universal acceptance of the genuine risks and opportunities associated with cyber security. One Australian Security Summit participant relayed a somewhat extreme quote from a senior Australian business leader. In response to a briefing on the Target breach in the US that saw the resignation of its President and CEO, the Australian executive noted with relief "…I am glad they (major breaches) do not happen here, like they do in America!" Hopefully this somewhat unbelievable perspective is not reflective of Australia's broader C-level cohort. Yet KPMG's recent Global CEO Outlook 2015 survey revealed that over half of the CEOs surveyed do not feel fully prepared for a cyber event.

The practical efforts to realise this objective should be focused on first increasing board level of awareness of risks and opportunities, then ensuring there are the requisite tools/support available to enable organisations to help themselves.

[13] Winnefeld, J.A. Jr, Kirchoff, C. and Upton, D.M., Cybersecurity's Human Factor: Lessons from the Pentagon, Harvard Business Review, Sep 2015.

**Proposal 1: Expand the Prime Minister's Cyber Security Summit into a larger, annual event.** For the foreseeable future, the government-business interface of cyber security needs to be championed by the Prime Minister. An annual PM-led dialogue will force cyber security into the mainstream, providing the impetus to business and bureaucrats to overcome barriers to progress and increasingly focusing on the economic potential of the industry. Such a commitment will also provide a powerful leadership signal to federal ministers and the other tiers of government, for which cyber security should be an equally significant concern. An annual event could be supported by the Programme Office and co-funded by industry.

**Proposal 2: Establish a cycle of cyber security health checks for Australia's top companies,** before extending this initiative to priority government agencies and critical infrastructure suppliers. KPMG was one of the major contributors to a similar initiative pioneered in the UK. This Government sponsored activity increased the level of board attention on cyber security by assessing the cyber security health of the organisation and reporting this back to the board. It included an assessment of the firm relative to other leading companies to help inform the board's understanding and any investment decisions.

Cyber security health is not limited to an assessment of a company's technical cyber security systems but speaks to a holistic assessment of a company's cyber security preparedness and awareness. While there is a question if it should be mandatory, such an approach is likely to drive greater focus over the medium term and help drive the necessary culture shift at the board level and below. As was the case in the UK, a consortia of firms could carry out the health checks independently, before consolidating and anonymising the results. It is the anonymised results and high-level statistics that could be provided to both government and the participating organisations.

**Proposal 3: Endorse an adaptable standard of good cyber security.** Government can empower the private sector through the provision of authoritative knowledge. ASD's Top 35 strategies to mitigate cyber intrusions provides a foundation on which to develop a more digestible, adaptable and nationally-applicable standard. Government could work with the cyber security industry and relevant industry sectors to develop a matrix of practical steps, depending on desired level of protection and sector. A co-design and technology-agnostic standard would help it to be resistant to the rapidly changing threat environment. While endorsed by government, the standard should stop short of being a regulated standard – for now. International experience suggests regulation in this area is fraught and it is not clear the cost-benefit analysis would provide a conclusive result one way or the other. Introducing a mandatory standard (regulation) may be directly counterproductive to the pursuit of a collaborative and more open government-business relationship. A voluntary standard will enable more companies to opt in and provide a baseline of acceptable health. Government could encourage larger companies to demand smaller companies in the supply chain adhere, deepening the level of national protection and resilience.

**Proposal 4: Introduce a time-limited additional tax concession or incentive for improved cyber health.** The incentive could be targeted toward small-to-medium sized enterprises. Action could be validated or attested to by business owners and managers completing and submitting a checklist. Such action would incentivise greater management awareness and accountability, would enable businesses to promote an active approach to cyber security and support the development of a local cyber security industry by increasing overall national investment.

## Support the development of a local cyber security workforce and industry

The global cyber security market is worth more than A$100 billion in 2015, and is expected to exceed A$230 billion by 2020[14]. Australia should aggressively pursue an increased share of this market. It is an already crowded market place with established leaders and there is a growing pool of contenders from across the globe.

The measures included in the Innovation and Science Statement and the 2016 Defence White Paper signal the Government has recognised the importance of catalysing Australia's cyber security industry and local cyber security workforce. The Cyber Security Growth Centre, when coupled with initiatives such as equipping students to create and use digital technologies and establishing Data61 – Australia's Digital and Data Productivity Network, should act as a powerful signal to the private sector to invest more heavily in the cyber security sector and skills base.

Some commentators would argue government has no place in picking winners or propping-up a commercial sector. But cyber security is different in Australia as the government has a vested interest in increasing the domestic pool of internationally-credible cyber security providers. The leading national providers of cyber security solutions are housed in nations with activist governments. Indeed, the governments of US, UK and Israel actively support and promote their cyber security industries domestically and internationally. However, unlike the other proposed Work Streams, this is one where government could play a subordinate role, given the primary beneficiaries will ultimately be the private sector.

The development of a cyber workforce is an objective with primarily a market-based pursuit. The demand for cyber security skills must be more clearly articulated by the market – be it the government or private sector market. It is crucial for organisations of all sectors and types to comprehend the pervasiveness of cyber security. There is a need for lawyers, accountants, risk managers, executives, as well as cyber security practitioners to be able to address cyber security risks. This requires a collective effort to lift the skills of all Australians, particularly those with cyber responsibilities.

As noted above, the importance of a cyber workforce was well articulated in the 2016 Defence White Paper. A concerted focus in such a prominent national document should reinforce the very real demand for cyber security professionals. Some of the initiatives proposed below are closely aligned or complementary to those already announced by the Government.

**Proposal 1: Provide a small funding pool for the ACSC to partner with the research sector and private industry to support innovative cyber security start-ups.** The ACSC as it stands has an unparalleled insight into cyber security trends. As it matures, it should also have an increasingly close relationship to the broader cyber security needs of the Australian economy, making it well placed to identify innovative technical and business solutions. In deciding recipients for grants, the ACSC should partner with the tertiary sector and select industry partners. This initiative could be co-funded by Defence and the private sector, creating a similar model to those underway in the US, UK and Israel. The sums of money need not be large and could be complemented by a mentoring program from the ACSC and leading Australian companies.

**Proposal 2: Prioritise local cyber security companies and cloud service providers on regional trade missions.** Consistent with domestic growth objectives, the Cameron Government has actively supported the domestic and international growth of its cyber security industry. Relevant Australian Ministers at the federal and state level should take cyber security-specific delegations on trade missions to priority markets, particularly in the Indo-Pacific. This is a low-cost initiative that can start to shift the national business psyche by highlighting the potential and importance of cyber security to the Australian business community.

**Proposal 3: Support the growth and professionalisation of Australia's cyber security workforce.** A dearth of skilled cyber security practitioners has long been a complaint of the Australian business community. Seemingly the market is not correcting the skills shortage. While business can do more to help grow the pipeline, government can support a range of practical activities, including:

- creating a national accreditation;
- establishing a 12 month cyber security 'traineeship' through the ACSC and participating businesses that will provide participants with a recognised qualification/certification;
- ongoing promotion of STEM skills from the earliest stages of formal education;
- developing short courses for non-technical staff involved in responding to cyber incidents.

[14] Cyber Security Market Report: http://cybersecurityventures.com/cybersecurity-market-report/

## The way forward

The release of the Government's Cyber Security Strategy will provide the formal approval for government to start the genuine reform of Australia's approach to cyber security. But it will be up to business as much government as to how far and fast Australia goes. The opportunities are great. The imperatives are there. The greatest risk is inaction.

Now is the time for the Australian Government and the Australian business community to show leadership and commit resources to make a difference.

# Contact us

We welcome your feedback on our views and please feel free to contact us.


**Steve Clark**
**National Sector Leader,**
**Defence & National Security**
+61 3 9288 6937
steveclark@kpmg.com.au

**Anthony Court**
**Lead Partner, National Security**
+61 2 6248 1102
acourt@kpmg.com.au

**Mark Tims**
**Partner,**
**Technology Risk**
+61 2 9335 7619
mtims@kpmg.com.au

**Gordon Archibald**
**Partner, Cyber**
+61 2 9346 5530
garchibald@kpmg.com.au


**kpmg.com.au**





February 2016. CRT056006A. VICN13623LOB