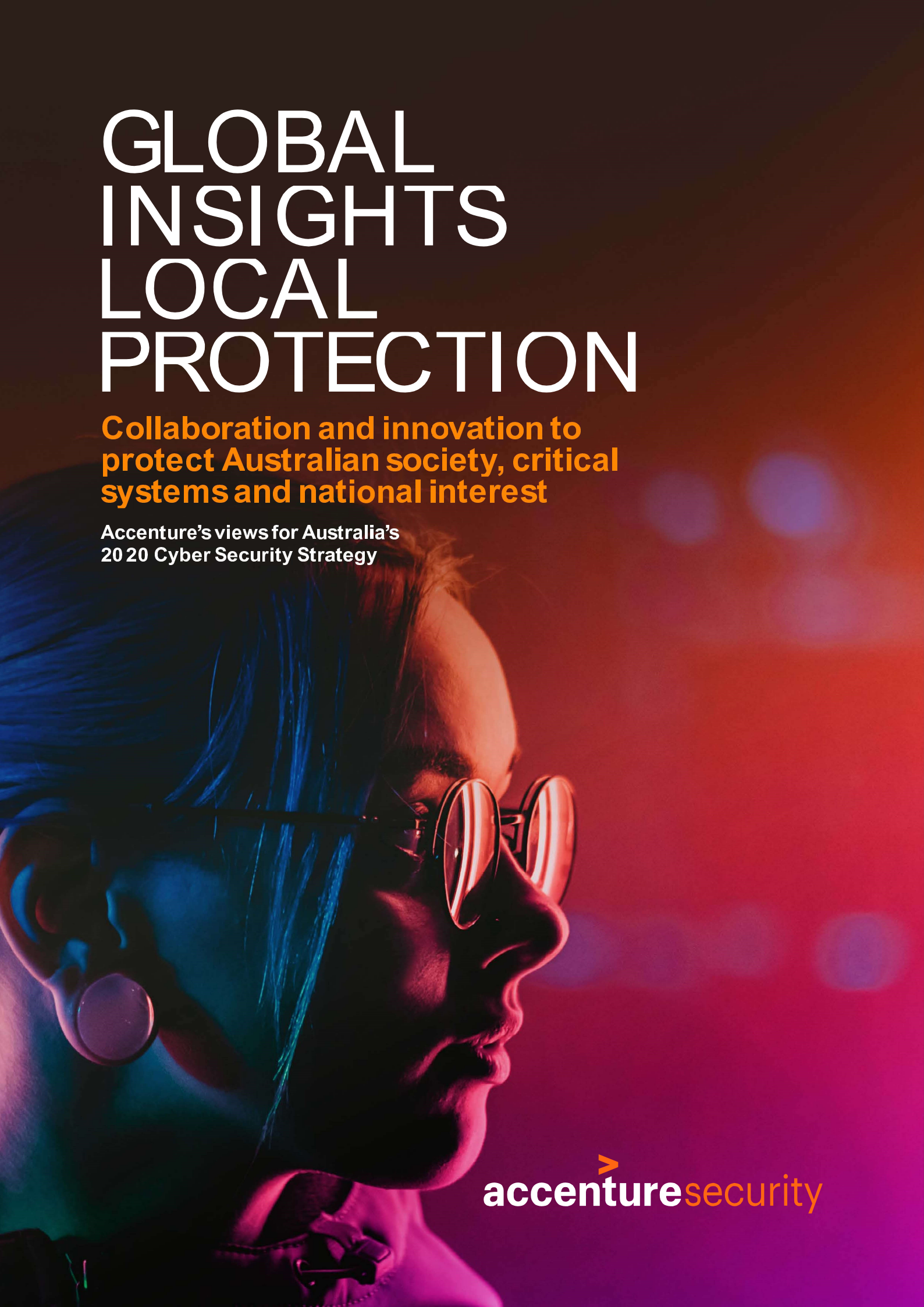
GLOBAL INSIGHTS LOCAL PROTECTION

Collaboration and innovation to protect Australian society, critical systems and national interest

Accenture's views for Australia's 2020 Cyber Security Strategy



accenturesecurity

Contents

Introduction and background

Accenture welcomes the opportunity to respond to the Department of Home Affairs Discussion Paper for Australia's 2020 Cyber Security Strategy. It is a critical time to review and plan for the evolving nature of cyber threats and prepare Australia to be cyber resilient. This will enable future growth and prosperity for the nation. As a professional services provider in cyber security, Accenture has an interest in this discussion. Our observations from partnering with our clients is that, unlike other organisational risk issues, cyber security is a global issue that will require a co-ordinated local response.

Throughout this response we will draw on Accenture research conducted in partnership with renowned security research organisations including the Ponemon Institute and Accenture's own iDefense. Lessons from engagements with governments and industy, puts Accenture in a unique position to contribute our observations on cyber security and its impact on organisations and society.

Through effective collaboration across Australia's dynamic digital ecosystem we believe cyber security can be embedded into the fabric of Australian society.

Executive summary

A modern and responsive cyber security strategy is an opportunity to maximise the prosperity and future growth of Australian society. While cyber security is a global issue, it necessitates a co-ordinated local response. Australia's 2020 Cyber Security Strategy will benefit from an innovative approach to partnering with industry and citizens, leveraging the global and local insights collaborators bring. Accenture's view is that a 'Cyber Council' is the appropriate collaboration mechanism, where members of the council share both risk and responsibility for Australia's cyber security agenda.

Not alone in a threatening world

The Australian Government has a responsibility to provide leadership in responding to any existing or emerging threats that have a material impact to:

- National security;
- Citizen safety (particularly to vulnerable citizens);
- Financial or economic national interests; and/or,
- Australian societal values.

However, the Australian Government is not alone in responding to these threats.

Introducing the 'Cyber Council'

A 'Cyber Council' approach addresses the above critical cyber threat issues by building common values into the cyber ecosystem and promotes information sharing as a key strategy for security. Through a council approach Australian government, industry and citizens can implement:

- Industry standards for technology hardening through shared technical expertise;
- Regulation approaches for government based on public good;
- Enforcement frameworks to assist the role of law enforcement in cyber security;
- Information sharing paradigm that focuses on specific and relevant threat intelligence; and/or,
- Engagement framework with the global community aiming to enhance cyber security.

A framework for growing confidently

Cyber threats will evolve,and the Australian Government will be empowered to respond actively with a framework co-created with industry and citizens. Key considerations for the development of a modern cyber framework include:

- **Humans first** – Using human centred approaches, including citizen segmentation, to tailor policies and interventions at citizen, business and industry levels;
- **Digital identity** - Providing Australians with a way to authenticate their digital identity via secure platform-based technology to underpin a strong digital economy;
- **Strategic maturity** – Developing intelligence-led and agile approaches for policy, strategy and management combined with integrating operations and security capabilities in 'Security Operations Centre' constructs to enhance cyber vigilance;
- **Global governance** – Maximising cross border collaborations on regulations for industries and supply chains to unite jurisdictions for security;
- **Technical maturity** – Utilising technical approaches including 'DevSecOps' and secure platforms to improve cyber security for systems;
- **Research and development** - Investing in research focused on Machine Learning and AI to increase proactive cyber monitoring. Additionally, preparing Australia for the disruption of emerging technology including paradigms like quantum-, nano- and biological computing;
- **Skills and capabilities** – Developing existing cyber security capabilities in workforces as well as innovating new capabilities like the proactive 'Cyber Ranger'; and,
- **Innovative partnership models** – Exploring government-private partnerships which leverage shared services, capabilities and funding to efficiently use limited resources and skills. For example, a 'capability retainer' partnership for cyber incident response.

Q1. What is your view of the cyber threat environment? What threats should Government be focusing on?

As Secretary Pezzullo stated in March 2019 in relation to issues of national security, including that of cyber security, "We have seen and dealt with these types of challenges before. What will challenge us in the 2020s will be their concurrency, confluence and interdependencies."[1] The nature and influence of the cyber security environment is evolving and posing more challenges and creating more opportunities for Australians.
The following outlines our view of the current cyber threat environment and considerations for the Australian Government.

1.1 Vulnerable targets

Whether by accident or intent, humans remain the biggest contributor to successful cyber breaches across organisations and industries. In 2018 Accenture published research in partnership with the Ponemon Institute (Michigan, USA) that found the two biggest contributors to cyber attacks for corporate organisations are accidental publication of confidential information, followed by internal attacks by disgruntled employees.[2] This research was conducted in a cross-section of companies where cyber security was a key concern for senior executives. If this data emerged from supposedly 'cyber savvy' workforces, it is easy to assume that there may be vulnerable sections of the community sitting as ready targets for malicious attacks.

1.1.1 Small businesses

As identified in the Australian 2020 Cyber Strategy Discussion Paper, Accenture agrees that small businesses are a vulnerable target for threat actors. The Chubb Security 2019 Cyber Risk Survey found that the cost of protecting individuals and companies from cyber attacks is increasing, and that fewer than 31 per cent of small business employees receive cyber security training.[16] Data released from a 2019 Verizon study indicated that 43 per cent of all successful Australian cyber attacks targeted small business employees.[5] Small businesses are important in and of themselves but they may also be a weak link in a larger supply chain.

1.1.2 Public institutions and intelligence assets

The second largest victim group identified in the Verizon 2019 study on cybercrime was public sector employees at 16 per cent of the successful attacks identified.[5]
In addition, cyberespionage data reveals that public institutions are targeted more than any other institutions.[9] The public sector and its infrastructure are attractive targets for cyber threat actors due to the centralised intelligence they often represent.

Data mining, inadvertent or ill-considered information sharing and the explosion of personal information shared by IoT devices enables large scale surveillance of public servants, defence and intelligence staff. The personal details of current and future public officials are a valuable commodity. The collection of data on these groups can inform insider threat actors and provide opportunity for blackmail and coercion operations.

Importantly, the different roles and responsibilities of state and federal government have relevant implications. Data collected from government agencies across the USA in 2016[9] showed that federal agencies differ dramatically from state and local participants in their ability to respond to cyber threats. For example, nearly 45 per cent of state and local government respondents express confidence in their organisation's ability to monitor for breaches, while far fewer federal survey-takers agree. Part of this difference could reflect the much greater scale of federal digital networks, but another element is likely to be a greater realisation at the federal level that successfully monitoring for breaches can be an extremely difficult undertaking.[9]

1.1.3 Cyber security as a public health issue

A significant and growing component of worldwide cyber security is the threat that some individuals pose to themselves or others through their vulnerability to cyber attack.[9] Natalie Ebner et al (2018) identified that demographic risk factors for cyber fraud-related activities include low socioeconomic status, large household size, and ethnicity.[4] Mental health is also associated with an individual's susceptibility to cyber attacks, with a growing body of evidence showing that those with depression are more susceptible to online fraud techniques.[4] This frames the profile of cyber threats in line with public health threats. Just as there are vulnerable populations for public health concerns, we see this mirrored in vulnerable targets for cyber security attacks.

Cyber security threats are invisible until the point of impact, often posing a risk not only to the targeted or 'infected' individuals but also to others who are at risk of secondary exposures to a contagion.[8] A public health view may be relevant when developing frameworks for cyber security responses. The following vulnerable communities are those that Accenture believes need consideration from the Australian Government when considering the cyber threat environment.

1.1.3.1 Ageing population

As the rate of internet adoption by older Australians increases, so too does the rate at which this population is targeted by malicious cyber attacks. Reasons for this include a lack of confidence older adults feel when engaging with the internet, coupled with reducing decision-making capacity and decreased sensitivity to social cues of deception.[4] Threat actors are aware of this, with attackers increasingly using age-tailored online approaches to target this group. Natalie Ebner et al in their research research published in 2018, also found that susceptibility to cyber attacks increases with the loss of loved-ones, illness, limited mobility and low levels of social interaction.[4] These factors compound this group's vulnerability.

1.1.3.2 Adolescents and young adults

Adolescents and those emerging into adulthood are another susceptible population, partly due to the volume of people in this group using the internet. Evidence suggests that there is increased phishing sensitivity in millennials aged between 16-25 years. Young adults are more vulnerable than their Gen Y counterparts.[3] This age group is also one of the biggest consumers of social media, creating a pool of potential targets of attacks via social applications. For example, the 2016 Snapchat data leakage from a phishing attack or disinformation distributed via social media.

1.1.3.3 Those with intellectual disabilities

Citizens living with intellectual disabilities are increasingly connected to cyber space.[17] They use social media to connect with peers and communities and there is increasing use of connected medical and support devices to enable this population's independence and support. Caton and Chapman in their 2016 research found while many aspects of digital connection have positive impacts, this population remains at risk of cybercrime due to reduced cognitive function and inability to pick up on social cues of deception.[17] Accenture notes there is little focus on the education of this population and their carers and believes the Australian Government should consider this in its approach to the 2020 Cyber Security Strategy.

1.2 The cyber threat landscape

Annually the Accenture iDefense threat intelligence team create '*The Cyber Threatscape Report*' which presents key findings from research into significant cyber threat trends. The most recent report covers observations from January 2019 until July 2019.[7] An overview of the findings relevant for this response can be found at Appendix A.

The annual report aims to inform IT security teams, business operations teams, and organisations' leadership about emerging cyber trends and threats, to help those groups anticipate key cyber security developments. Accenture iDefense threat intelligence has been creating relevant, timely and actionable threat intelligence for 20 years.

1.3 Threat trends in focus

1.3.1 Geopolitics and cyber security

One of the great challenges of 2020 and beyond will be responding to attempts by foreign powers to disrupt critical technology systems. As opportunists, threat actors can capitalise on the impact of political and other high-profile events to exploit legal changes, price swings or international geopolitical manoeuvring that occur in and around these events. In addition, a foreign country may use cyber attacks to influence decision making and change behaviours in targeted nations.[7] Geopolitical uses of cyber enabled information operations can include an offensive cyber attack aimed to create psychological effects in a target population and influence national decisions.[7]

1.3.2 Supply chain and third-party risk

Extended supply chain threats are growing. While some organisations and industries have successfully built resilience against cyber attacks, threat actors are adapting and shifting their attack patterns to exploit third- and fourth-party supply chain partner environments to gain entry to target systems.[7]

The traditional boundaries of attack surfaces are shifting as suppliers, partners and managed service providers integrate with organisations' business processes and infrastructure. For example, the use of open-source code is common in many Australian Government systems. Use of open-source code is not prohibited by the Information Security Manual and is a cheap and effective way to rapidly develop software or augment systems. Open-source code is rarely subject to the needed level of security focused testing and auditing including vulnerability assessments. This represents a significant vulnerability in supply chain security. The United States have pioneered the use of a 'Software Bill of Materials' for use in system documentation to guide investigators if a security incident occurs—the incorporation of this into system documentation for Australian systems would assist recovery or even avoidance of a zero-day incident associated with open-source code use.

1.3.3 Syndicated cybercrime

Conventional cybercrime operations continued to be active during 2019, with actors sharing document builders and malware for use in crimeware campaigns and targeted intrusions. But there is a new level of resilience and maturity in organised cybercrime as, due to high-profile law enforcement actions,[7] crimeware groups shift their operating models from open partnerships on underground forums to close-knit syndicates.

1.3.4 Cloud infrastructure

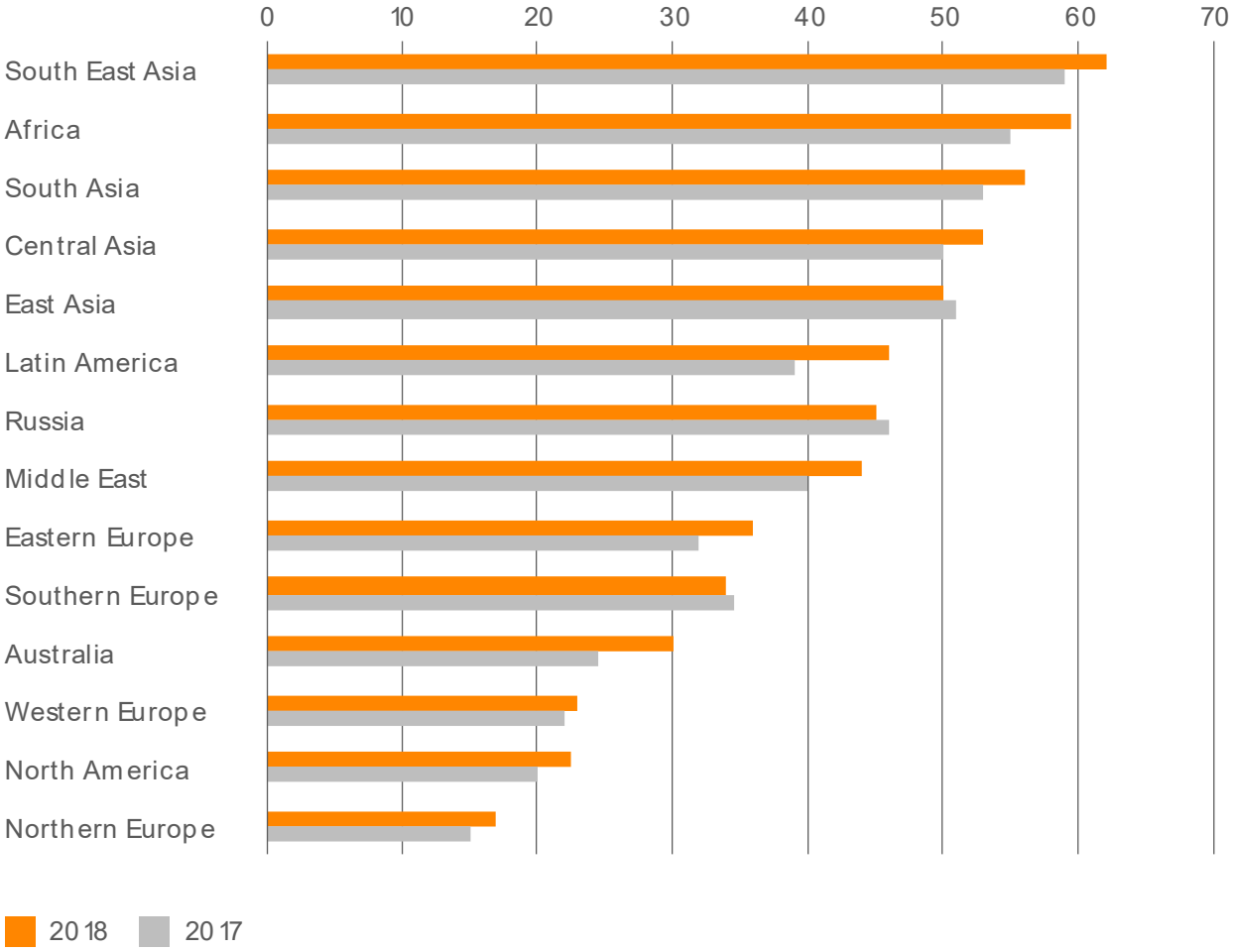
It is estimated that 83 per cent of enterprise workloads will move to the cloud by the year 2020.[12] This pivot to the cloud has prompted security researchers and threat actors to look for vulnerabilities in cloud infrastructure.[7] Multi-tenant public cloud providers are ideal targets for exploitation of side-channel CPU vulnerabilities, as shown by the recent releases of Meltdown and Spectre bugs that target physical processing. This further compounds the vulnerability of small to medium-sized businesses who largely rely on shared cloud systems for their operations.[13]

1.3.5 Securing critical infrastructure in the Asia Pacific region

Data collected in a 2018 Accenture commissioned report '*Securing Critical Infrastructure*' found that the South-East Asia region had the highest number of attacks on their infrastructure assets.[6] Australia was impacted by less than half of the volume of attacks as those to our north and west. Attacks on one nation affect others due to the importance of regional resources trade.

As a regionally significant exporter of coal, oil and gas, an attack on an Australian exporter could disrupt the ability of regional partners (such as Japan) to manage domestic needs. The inability of Australia to service the Japanese gas market, for example, could force Japan to seek other suppliers at prohibitive cost. The ability to use such an attack to apply pressure to other nations for political outcomes should not be overlooked.

Figure 1: Volume (by per cent) of cyber attack on infrastructure assets by region



1.4 The digital identity crisis

Individual identity is fundamental to society. As we increasingly move economic and social transactions into the digital domain, the challenge of authenticating identity grows significantly. Currently individuals use a variety of different identities when they interact with the digital world, such as email, usernames, browser history and Facebook profile. This fragments an individual's identity throughout the digital ecosystem and impacts the ability of government and service providers to reliably ensure that services are provided to the right people. Conversely, internet users have less ability to validate the author and substance of digital content. For example, Facebook recently closed 14 per cent of all accounts in 2018 after identifying that they were fake.[15]

Malicious threat actors can easily monopolise fragmented digital identity as it makes it extremely difficult to attribute attacks.[8] This places Australia's digital economy at risk. Providing citizens a secure way to authenticate their identity needs to be the foundation of the Australian Government's approach to Australian cyber security. We discuss mechanisms for this in Question 8, 'Digital identity-as-a-platform.'

1.5 Future thinking- quantum, nano and biological computing

While not directly impacting the current cyber threat level, it is essential for government and industry to think about the second and third horizons of cyber threats: emerging computing paradigms. These paradigms include:[10]

- Nanocomputing;
- Quantum computing;
- Biological or genome-based computing; and,
- Increasingly evolving system and network architectures.

These future technologies are likely to disrupt cyber security in a matter of years. New and innovative approaches to cyber security will be needed to combat the potential threats these technologies pose. Investing in research focusing on cyber security in these areas will be important to prepare Australian society for the future. Quantum computing alone, with the ability to confer quantum encryption, will render all current forms of encryption redundant.[10]

1.6 What threats should government focus on?

It is Accenture's view that the Australian Government should provide leadership and responsibility for helping to respond to any existing or emerging threats that have a material impact on national security, citizen safety, a financial or economic impact on the nation or seek to materially disrupt Australian societal values. As cyber threats and threat actors will continue to evolve, the Australian Government would be more empowered to respond to any threat with a well-defined threat impact framework that is co-created with key stakeholders across Australia.
As discussed throughout our response to Question 1, cyber security is a global issue that requires co-ordinated approaches to mitigate impacts and develop solutions. The Australian Government cannot manage these risks alone and will benefit from seeking new and emerging models to engage with businesses, industries and citizens to co-ordinate Australia's Cyber Security Strategy.

References for Q1

[1] Michael Pezzullo's seven gathering storms: national security in the 2020s, March 13, 2019, Michael Pezzullo. https://www.themandarin.com.au/105494-michael-pezzullos-seven-gathering-storms-national-security-in-the-2020s

[2] 2018 State of Cyber Resilience, Accenture. https://www.accenture.com/in-en/insights/security/2018-state-of-cyber-resilience-index

[3] Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behaviour, 2018, Weems et al, PLOS:ONE. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207408

[4] Uncovering Susceptibility Risk to Online Deception in Aging, 2018, Natalie Ebner, Daniela Oliveira et al. http://www.daniela.ece.ufl.edu/Research_files/gerontology18.pdf

[5] 2019 Data Breach Investigation Report, 2019, Verizon. https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings

[6] Securing Critical Infrastructure, 2018, Accenture. Securing Critical Infrastructure, 2018, Accenture. https://www.accenture.com/t00010101t000000z__w__/au-en/_acnmedia/pdf-96/accenture-securing-critical-infrastructure-new.pdf

[7] iDefense Cyber Threatscape report, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

[8] Is a public health framework the cure for cyber security?, 2012, Brent Rowe, Michael Halpern, Tony Lentz. https://www.rti.org/sites/default/files/resources/rti-publication-file-7123c5de-0877-4114-8700-01dc8a94f8cc.pdf

[9] Accenture High Performance Security Report, 2016, Accenture. https://www.accenture.com/_acnmedia/pdf-37/accenture-confidence-capability-rebooting-public-sector-cybersecurity-research.pdf

[10] Security Outlook: Six Cyber Game Changers for the Next 15 Years, 2014, Patrick McDaniel, Alexander Swami. http://patrickmcdaniel.org/pubs/ieeecom14.pdf

[11] Protecting our digital heritage in the age of cyber threats, December 6 2018, Stanley Shanapinda. https://www.themandarin.com.au/102366-protecting-our-digital-heritage-in-the-age-of-cyber-threats

[12] 83 Per cent Of Enterprise Workloads Will Be In The Cloud By 2020, January 7, 2018, Louis Columbus. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#3d0abe4d6261

[13] The CPU catastrophe will hit hardest in the cloud, January 4, 2018, Russell Brandom. https://www.theverge.com/2018/1/4/16850120/meltdown-spectre-vulnerability-cloud-aws-google-cpu

[14] Australian Cyber Security Centre, 2017, ACSC. https://www.cyber.gov.au/publications/acsc-threat-report-2017

[15] Securing the digital economy: reinventing the internet for trust, 2019, Accenture. https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

[16] Chubb Cyber Risk Survey 2019 Executive Summary, 2019, Chubb Security. https://www.chubb.com/us-en/individuals-families/agent-marketing/online-you-protected/pdf/Chubb_Cyber_Survey.pdf

[17] The use of social media and people will intellectual disability: A systematic review and thematic analysis, 2016, Sue Caton and Melanie Chapman. https://www.tandfonline.com/doi/abs/10.3109/13668250.2016.1153052

Q2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy? And Q3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

It is important that government, industry and individuals are pragmatic when it comes to determining who is responsible for managing cyber security. Policy and legislation may be required to provide minimum baseline security controls for all businesses, but security will ultimately hinge on the collective action of all individuals.

2.1 Current responsibility matrix

Using the information provided by the Department in its 2020 Cyber Strategy discussion paper Accenture has analysed the current responsibilities of stakeholders and outlined these in Table 1.

Table 1: Current responsibility matrix for cyber security in Australian society

Responsibility	Federal Government	State Government	Industry	Business	Individual
Policy/regulation development	x	x			
Enforcement/ Incentives	x*	x*			
Education/ Training	x	x	x	x	
Reporting incidents to government			x	x	x
Information sharing	x	x	x	x	x
Protecting internal systems to the organisation	x	x	x	x	
Protecting individual assets – computers, phones etc.	x	x	x	x	x

*Enforcement through federal and state police

It is important for responsibility to be clear across stakeholders. However, responsibility does not equal action. To empower stakeholders in these roles to act, government needs to engage innovatively with industry and citizens.[2]

2.2 Introducing the 'Cyber Council'

The growing view of leaders in 2019 is that the best approach to cyber security responsibility is continuous collective action.[4] The development and enforcement of cyber security regulation needs to be carried out in concert with key stakeholders across industry, government and citizens stakeholders.[2] Leaders from across organisations and governments need to be aligned with the cyber community, rather than focused on the digital footprint of their own organisation.[4] The structure for this co-design will be critical for successful outcomes.

Accenture recommends the formation of an Australian 'Cyber Council,' which would be a collective of key representatives from across stakeholder groups that can together develop and defend an holistic approach to Australian cyber security. A benefit of this approach is that it shifts the paradigm away from transactional organisation-to-government information sharing which, as discussed in Question 21, has challenges to overcome. A 'Cyber Council' approach will build common values into the ecosystem, intrinsically building trust and prompting information sharing as a key strategy for security.

2.2.1 Bringing the Cyber Council to life

The Cyber Council provides an effective construct for industry, citizen and Government to share risk and responsibility in defining and responding to Australia's cyber security needs. Benefitting from a diversity of views and experiences, a Cyber Council construct enables the complexities of cyber security to be addressed holistically.

Key outcomes for the 'Cyber Council' would be to:

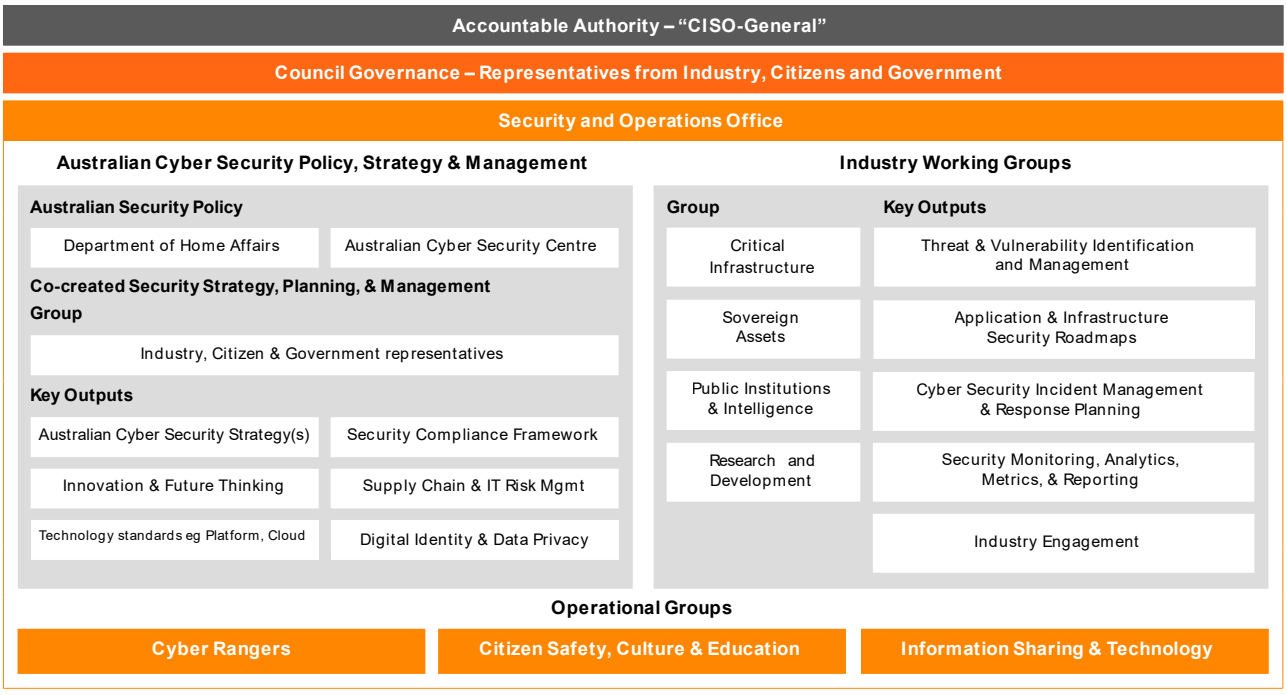
- Provide industry based standards for technology hardening through shared knowledge and technical expertise;
- Shape cyber regulation approaches for the Australian Government based on public good;
- Develop enforcement frameworks to assist the role of law enforcement in cyber security;
- Share specific and relevant threat intelligence that may a material impact to the nation; and,
- Engage with and be Australia's representative for global governance of cyber security.

2.2.2 Approaching an operational model for the Cyber Council

Leadership of the Council requires an Accountable Authority such as a 'CISO-General' appointed through a competitive process. Supporting the Accountable Authority is a leadership team consisting of representatives from industry, government and citizens. These representatives will be supported by an operating model that aligns members on intent through to execution. We present Accenture's indicative approach to a Cyber Council operational model in Figure 2.

Although governance and strategies would be co-created in the Cyber Council, the relevant Government authorities would retain ultimate ownership of policies and regulations. Key outputs of the Cyber Council will be developed by Industry Working Groups, grouped by the critical systems they manage; Critical Infrastructure, Sovereign Assets, Public Institutions and Intelligence and Research and Development. The Cyber Council strategy and vision will benefit from a strategically agile approach where cycles of plan, implement, observe and iterate occur regularly guided by the collaborative leadership of industry, citizen and Government.

Figure 2: Illustrative Cyber Council operating model



* Potentially leveraging the infrastructure of the ACSC, re-defining the role to be the operational arm of the Australian Cyber Council

2.2.3 Operational groups

The operational arm of the Cyber Council includes an innovative capability, the Cyber Ranger. A Cyber Ranger team consists of cyber professionals able to proactively manage Australia's connected cyber space. This capability is discussed further in our response to Question 17. The second operational capability focusses on the culture change required to bring Australian citizens in-line with the evolving nature of cyber security. The final operational capability will support information sharing through technology enablement including ongoing support through the Information and Technology operational group.

2.2.4 Success factors for an effective Cyber Council

The formation and sustainment of a Cyber Council will require commitment from all key stakeholders involved. Accenture recommends the following to be considered:

- Members of the Cyber Council dedicate full time to the responsibilities of the Council. Appointment terms and job mobility models should be established;
- Investment must be spread across contributors (whether in capital, in-kind or fee-based) depending on the nature of the stakeholder and their abilities to contribute;
- Leveraging existing structures like the Australian Cyber Security Centre, which already acts as a data collection point for citizens, will jump start the operational capabilities of a Cyber Council model; and,
- Maximise the presence of global organisations, that already span jurisdictions and industries, and can provide global views on cyber security to bring immediate value to the Australian agenda.

‘Cyber Council’ case study – Singapore

The Singaporean Government has initiated a similar concept, collaborating with the Global Resilience Federation Asia Pacific (GRF APAC) and launching the OT Cybersecurity Information Sharing and Analysis Center (OT-ISAC) on 1st October 2019. The OT-ISAC includes representatives from government, critical industry and critical information organisations. The aim of OT-ISAC is to build trust between parties, promote safe and secure information sharing, build local OT cyber security analytics and response competencies and foster cross-border cooperation on OT cyber security. One of the strengths of the OT-ISAC is the depth and breadth of experience and expertise that can be leveraged to create a capability that scans for and responds to cyber threats.[5]

‘Cyber Council’ case study – Japan

The Japanese Government have taken steps towards a ‘Cyber Council’ construct establishing the Japan Cybersecurity Innovation Committee (JCIC). Directors of the JCIC include university professors, policy experts, industry leaders and Accenture’s Managing Director for Security in Japan. JCIC leadership cite the following as the basis for the formation of the committee “Japan …(is seeking)… human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspace and physical space.”[8]

2.3 Government powers

Currently both the Australian Government and industry are struggling with the lack of Government mandate to influence the industry approach to cyber security, particularly for critical systems. The natural step is to review the Australian Government’s current powers in relation to cyber security as a common good and determine what needs to change. This is particularly hard for cyber security and many nations have been grappling with the right way to influence the cyber security agenda.[3] We discuss this in detail in Question 4.

2.4 Role of custodian

When moving to an information sharing paradigm, the protection of confidential information will be critical to the future role of government. The Australian Government is already demonstrating maturity in this area, appointing a National Data Commissioner in 2018.[6] Consideration to the complexity of holding of sensitive data must be a priority for the Australian Government.

2.5 Approach using citizen segmentation

A citizen segmentation approach would allow government to identify and group citizens on key cyber characteristics in their online activity and determine which groups represents a high degree of cyber risk. Personalised interventions or awareness campaigns tailored for these segments can then take place. In this way the Australian Government can maximise turning responsibility into action by targeting those most likely to pose a critical risk to Australian Cyber Security.

2.6 Corporate accountability

In 2017, Accenture research found that among 2,000 security executives across 12 industries and 15 countries, 70 per cent of the respondents agreed that "cyber security at our organisation is a board-level concern and supported by our highest-level executives." However, this study also showed that less than 35 per cent of board members feel prepared to respond to cyber incidents in their organisation.[7] These results speak to low levels of effective board engagement with cyber security, even though awareness is high. It also highlights board members' low level of capability to engage adequately with cyber risk. Just like any other corporate risks, cyber security should be key to the board's responsibilities and be part of mandatory audit processes. Mandating a board-level responsibility for organisational risk from cyber threat will increase board members' engagement with cyber security and improve an organisation's overall cyber risk profile.

References for Q2 and Q3

1 Weber Coercion in cybersecurity: What public health models reveal; Journal of Cybersecurity, 2017, Steven Weber. https://academic.oup.com/cybersecurity/article/3/3/173/3836936

2 The Regulation of Public Goods, 2004, Peter Dahos. https://www.anu.edu.au/fellows/pdrahos/articles/pdfs/2004regulationpublicgoods.pdf

3 We must treat cybersecurity as a public good. Here's why, 2019, Mariarosario Taddeo, Francesca Bosco. https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good

4 Is a public health framework the cure for cyber security?, 2012, Brent Rowe, Michael Halpern, Tony Lentz. https://www.rti.org/sites/default/files/resources/rti-publication-file-7123c5de-0877-4114-8700-01dc8a94f8cc.pdf

5 Singapore's Operational Technology Cybersecurity Masterplan, 2019, Cyber Security Agency of Singapore. https://www.csa.gov.sg/~/media/csa/documents/publications/ot_masterplan/otcybersecuritymasterplan.pdf

6 National Data Commissioner, Department of the Prime Minister and Cabinet. https://www.pmc.gov.au/public-data/national-data-commissioner

7 The Cyber-Committed CEO and Board, 2017, Accenture. https://www.accenture.com/_acnmedia/pdf-42/accenture-cyber-committed-ceo-and-board-pov.pdf

8 Japan Cybersecurity Innovation Committee, 2017, Toshinori Kajiura. https://www.j-cic.com/en/about.html

Q4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

Cyber security is a crucial public good for digitally-connected nations. These nations rely on government leadership to promote economic and social prosperity through the digital economy. Government must provide leadership in responding to any existing threats that impact national security, critical infrastructure or major impact to the Australian economy. Outlined below are some key considerations for the development of Australian Cyber Security Strategy.

4.1 Global developments

Globally, nations including Australian allies are embracing a more assertive and integrated cyber posture to manage the threat environment. From the establishment of Digital Embassies by Estonia to the creation of the Integrated Cyber Command by the United States (U.S.), nations are developing a centralised, integrated cyber capability and innovative resilience measures to manage the threat to data security.

4.1.1 Responding to myriad attacks

The U.S. Integrated Cyber Command reflects the need for the U.S. to achieve inter-operability with allied and like-minded nations in combating cyber threats. The command achieves a centralisation of cyber capability across disparate U.S. agencies. Additionally, it aims to leverage different skills and capabilities under one roof. This overcomes one of the principle issues of managing a national cyber capability, a challenge also shared by Australia. Co-ordination, centralisation and integration of services is a key way governments can fend off cyber threat.

4.1.2 Achieving resilience, redundancy and recoverability

Compared to the U.S., Estonia experiences significantly higher risk of physical and cyber attack. In response, Estonia has created a data embassy securely containing all the data related to national critical systems. This mitigates risk of a physical or cyber attack by creating a measure to verify data authenticity and easily identify any data that may have been interfered with.

Australia must make best use of the limited resources and skills in cyber security. Intelligent centralisation of capabilities and/or data are demonstrated ways of achieving resilience - shown through the experiences in the U.S. and Estonia.

4.2 Threat and risk management models for government to consider

4.2.1 National security

The Australian Government's National Security Agenda outlines the role of Australian Government to detect, prevent and respond to events and developments threatening national security. Table 2 compares how this may play out in responses to serious cyber threats.

Table 2: Government role in national security and potential parallels to cyber security role

	National security role	Potential cyber security role
Operations	Maintaining counter-terrorism capabilities and national coordination arrangements	Maintaining national co-ordination arrangements. Co-ordinating cyber security expertise at times of crisis
Policy	Maintaining national policies, legislation and plans	Maintaining national policies and legislation. Partnering with 'Cyber Council' on plans
Prevention strategy	Determining Australian Government prevention strategies and operational responses to threats	Collaborate with 'Cyber Council' to determine cyber attack prevention strategies and co-ordinate operational response to threats
Supporting States and Territories	Supporting the states and territories in responding to terrorist situations in their jurisdictions	Supporting the states and territories in responding to cyber attack situations in their jurisdictions
Critical response	Co-ordinated response to national threats - in such situations the Australian Government would determine policies and broad strategies in close consultation with affected states or territories	Co-ordinated response to national threats - in such situations the Australian Government would determine policies and broad strategies in close consultation with affected organisations or entities

4.2.2 Public health

It is useful to consider the government's role in managing public health risk as a metaphor for its potential role in cyber security. Like public health threats, cyber threats are often carried by 'infectious' vectors that, once exposed, can spread rapidly.[6] In addition, those most vulnerable to public health risks are also similarly vulnerable to cyber threats. Thus, another way for government to consider its role in cyber security is via the three prevention strategies outlined for public health.[7] Table 3 displays these and provides an example of a similar initiative for cyber security.

4.2.3 Cyber security as a public good

The Australian Government can leverage current thinking around public good regulation to inform the 2020 Cyber Security Strategy.[1] Arguably, cyber security is a 'global public good' with no single provider but rather a series of imperfect multilateral institutions.[8] As such there is a clear role for government to both fund initiatives and enforce cyber security relevant activities. This increasingly takes place with reference to global standards and/or collaboration.[8]

Table 3: Prevention strategies for Australian cyber security aligned to public health paradigm

	Public health example	Cyber security example
Primary prevention: addressing a potential threat before it can affect an individual	Public health campaigns at general practices	Cyber threat awareness campaigns targeted via citizen segmentation via short videos distributed on social media
Secondary prevention: responding to a threat after an individual has been affected but before an adverse impact of the threat has developed	Quarantining the area	Work with organisations/ individuals affected to prevent spread – One-time or short-term interventions
Tertiary prevention: intervening after an adverse impact of a threat has developed to prevent worsening of the impact	Medical aid to affected individuals	Potential civil/criminal penalties Intervention to manage threat supported by government

The advantage of government managing cyber security as a public good is that it promotes private industry and citizen collaboration due to common societal values.[1] Private actors and citizens remain profoundly important in the generation of, and adherence to, standards that promote public good.[2] While no existing model will completely align to the unique challenge of cyber security, lessons learned from public good may guide the right approach when managing cyber security risk.

4.3 Regulation and public policy

Progress in cyber security policy has lagged relative to the progress of the threat. Challenges to regulating cyber security include, tensions between civil liberties and security, geographical complexity and the jurisdiction variations between countries.[2] However, the Australian National University has found there is a significant appetite from citizens for public policy in matters of citizen safety.[3] It is imperative that the Australian Government evolve legislation in relation to cyber security and below are Accenture's recommendations to mature cyber public policy.

4.3.1 Global policy and enforcement

Policy decisions made to protect sovereign interests may have ramifications in Australia's ability to trade, collaborate and participate in a global digital economy. For example, Europe's General Data Protection Regulation (GDPR) has a global impact. Products (primarily software) that are sold to a global market must be customised to these 'localised' regulations. Maximising the global collaboration structures such as the United Nations will be important to explore as the Australian Government seeks to address the policy aspect of cyber security.

Law enforcement of cyber crimes will require global co-ordination. Australia will likely have to leverage global partners through structures like the Australian Cyber Security Centre (ACSC), or as described above a 'Cyber Council', in order to share information, conduct joint investigations, and foster a higher level of cyber security and resilience globally.

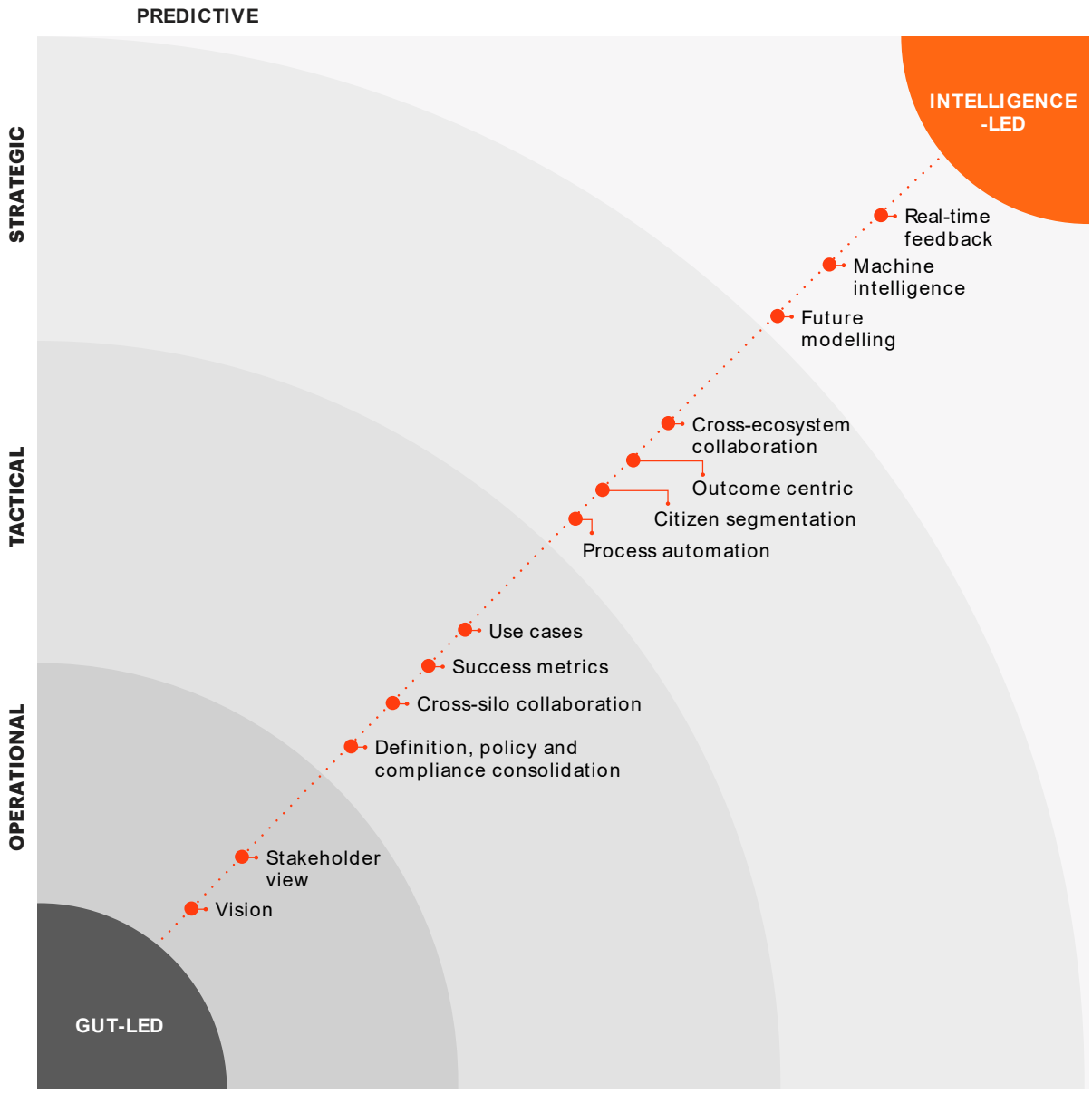
4.3.2 Intelligence-led policy design

An emerging approach to policy is intelligence-led policy design. The simplest form of intelligence-led policy design leverages historical data to inform policy decisions. The most advanced uses artificial intelligence modelling to dissect and design policies tailored to a broad range of variables.[11]

Figure 3 below demonstrates the steps governments can take to move towards truly intelligence-led policy design.

The impact of intelligence-led policy design is that the balances between penalties and incentives playing out over time and with differing citizens segments can be mapped and visualised before the policy is implemented. This will also maximise the intended impact across society for each policy.

Figure 3: Accenture's view on steps towards intelligence-led policy design



4.3.3 Citizen segmentation for policies

Australian National University released results in their '*Attitudes to national security: balancing safety and privacy*' research that found Australian citizens are comfortable about the Australian Government collecting internet and phone data in the name of national security.[3] However, government has a duty of care to balance this with individual civil liberties.[3] Just like policy-makers in cyber security, policy-makers in Australian healthcare are grappling with the need to evolve the systems, policies and strategies to meet the changing world while allowing citizens maximum autonomy and privacy over their health data.[3] An approach that is showing promise is citizen segmentation for policy design. Just as tailored interventions to citizens can improve overall cyber safety for Australia, tailored policies that meet individuals' circumstances will maximise compliance and engagement between citizens and their government.

Case study

In 2017 Accenture partnered with Longitude Research to survey over 2000 Australian citizens and use a data-driven approach to population segmentation. The outcome of this research revealed variables that we could reliably associate and helped health organisations understand what drives behaviour and preferences towards technologies. Learning from this, a growing body of evidence shows that policy design tailored to citizen segmentation has a better impact on cyber security-related behaviour than when policies or interventions are generalised.[4]

4.4 Government-held capabilities

A key consideration for the Australian Government will be what capabilities to develop and maintain internally. There are some situations where the Australian Government is uniquely well-placed to hold the capability and devolving it would be at odds with the aim of improving cyber security in Australia.

4.4.1 Response capability at times of crisis

For times of national crisis, the role of government to co-ordinate the response to an event is critical. It is also an area where the Australian Government has a strong existing framework. A cyber attack on critical infrastructure can quickly evolve from a cyber to a real-world event. In this instance national crisis frameworks apply, as for any crisis event that has societal impact. Lessons learned about whole of government crisis management include:[10]

- Plan early and test the plan;
- Establish clear leadership;
- Define roles of all players early;
- Use formal chains of command; and,
- Ensure strong public affairs management.

The Australian Government would do well to leverage expertise in national crisis management and control to find a similar role in cyber events.

In addition to crisis response the co-ordination of threat management is needed. However, most security technologists able to detect, diagnose and respond to a cyber attack are found in private industry. So, while the government is well-placed to manage the crisis response, the treatment and management of the existing and ongoing cyber threat may be better served by an ecosystem capability.

Considerations for government are to establish core agreements with capability partners who are response-ready. Another option to consider is government retainer agreements with cyber security specialists for service-level response to crises. These options are discussed further in our response to Question 9.

Case study - Maroochy Shire (QLD) sewage spill

In the early 2000's a QLD worker was turned down for a job at a sewage plant. This provided motivation for this internal threat actor to use a wireless radio transmitter to remotely break into the sewage treatment system and alter electronic data on the Supervisory Control and Data Acquisition system (SCADA) controller for the pumping station. This caused malfunctions leading to 800,000 litres of raw sewage being dumped into local rivers and parks. Post-event analysis has found that the City Council could have developed an emergency plan that would reduce the impact of such release at a faster rate[12] and that the council's role in the response is imperative for citizen safety and comfort.

References for Q4

[1] We must treat cybersecurity as a public good. Here's why, 22 August 2019, Mariarosaria Taddeo, Francesca Bosco. https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good

[2] At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, 2014, National Research Council. https://www.nap.edu/read/18749/chapter/3#15

[3] Attitudes To National Security: Balancing Safety and Privacy, July 2016, Jill Sheppard, Amin Saikal, Ms Katja Theodorakis. https://csrm.cass.anu.edu.au/sites/default/files/docs/2019/8/ANUpoll-22-Security_0.pdf

[4] Reimaging Australian Digital Healthcare, 2017, Accenture. https://www.accenture.com/_acnmedia/pdf-60/accenture-health-patient-centred-survey-au.pdf

[5] Segmentation analysis of susceptibility to cybercrime: exploring individual differences in information security awareness and personality factors, 2018, Lee Hadlington, Sally Chivers. http://irep.ntu.ac.uk/id/eprint/37546

[6] iDefense Cyber Threatscape report, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

[7] Weber Coercion in cybersecurity: What public health models reveal; Journal of Cybersecurity, 2017, Steven Weber. https://academic.oup.com/cybersecurity/article/3/3/173/3836936

[8] Is a public health framework the cure for cyber security?, 2012, Brent Rowe, Michael Halpern, Tony Lentz. https://www.rti.org/sites/default/files/resources/rti-publication-file-7123c5de-0877-4114-8700-01dc8a94f8cc.pdf

[9] The Regulation of Public Goods, 2004, Peter Dahos. https://www.anu.edu.au/fellows/pdrahos/articles/pdfs/2004regulationpublicgoods.pdf

[10] Managing crises and their consequences, 2018, Australian Public Service Commission. https://www.apsc.gov.au/7-managing-crises-and-their-consequences

[11] Becoming a data driven enterprise: Data industrialization, 2018, Accenture. https://www.accenture.com/_acnmedia/pdf-83/accenture-becoming-data-driven-enterprise-data-industrialization.pdf

[12] Cybersafety Analysis of the Maroochy Shire Sewage Spill, 2017, Nabil Sayfayn, Stuart Madnick. http://web.mit.edu/smadnick/www/wp/2017-09.pdf

Q5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

"Unless government leaders take effective action, there is a real danger that today's federal IT modernisation investments and efforts will be undermined by an erosion of public trust."

Gus Hunt, Accenture Federal Services
Cyber Security Lead

In 2017, Accenture Federal Services (Washington, U.S.), partnered with the U.S. Government Business Council to understand the impacts of digitisation on citizen trust in government. They found 77 per cent of federal respondents identified citizen trust in government as weak or weaker than ever.[2] This was supported by further research from the Pew Research Centre who determined that roughly half of Americans do not trust the American federal government to protect their data.[3]

It is Accenture's view that government-citizen trust has several critical dimensions. These are:[2]

- **Trust in delivery:** Citizens need fundamental trust in government and their agencies' ability to deliver services and solve problems as promised;
- **Trust in capability:** Citizens need specific trust in 'digital government' and an agency's ability to adequately safeguard personal, and often sensitive, information; and,
- **Autonomy to verify:** Citizens need to be able to verify through independent means that communications—email and text messages, websites, and phone calls or letters directing them to online sites—are indeed from real and trustworthy government sources.

Underpinning the success of all these dimensions is government-citizen engagement. How and what governments communicate to its citizens and the ability of citizens to respond is key to establishing trust. An effective citizen engagement strategy around cyber security requires government's transparency with citizens about 'what they are doing' and 'how they are doing it' regarding securing personal information and critical societal assets. Governments also need to provide avenues for citizens to respond with fears and concerns and to acknowledge the legitimacy of these concerns.

5.1 Approaches to building cyber trust equity

Initiatives such as governance efforts, collaborative relationships with industry and education campaigns are visible strategies that government leaders can enact to build cyber security trust with citizens.

5.1.1 Global governance

Visibility of governments' collaboration with global entities send clear signals to citizens of the seriousness nature of cyber security and the appropriateness of government response. Many forward-thinking governments are moving towards a global governance approach to cyber security. For example, cross border collaboration strategies form a key part of Singapore's recently released '*Operational Technology Cybersecurity Masterplan (2019)*'.[6]

In Question 3 we introduced the concept of a 'Cyber Council', an ecosystem of leaders that govern and guide Australia's cyber security measures. A way to enhance the validity of this

organisation or way of governing is by further engaging globally with thought leaders and credentialed global cyber security actors. One such avenue already available is the World Economic Forum's Centre for Cybersecurity. Launched in 2018, the Centre seeks to bring partners from "business, government, international organisations, academia and civil society to enhance and consolidate international security."[5]

5.1.2 Ethical code of conduct

The public needs assurance from their government that cyber strategies are aligned with broader social values. Just as pilots, doctors and construction workers require training in the ethical dilemmas and codes of conduct in their workplaces, this too should be a priority for any digital worker. The government's support and regulation of this code provides citizens with another indication of government's ability to keep them safe.

5.1.3 Proactivity and strength with key decisions

The Australian Government can proactively lead the cyber security agenda with a prompt and responsive strategy. Citizens look to government for a clear point of view on cyber security issues, from grassroots level through to industry standards. It is important for government to articulate a clear strategy to citizens. The following offer some ways to achieve this:[1,2,6]

- Appoint an accountable authority eg. a CISO-General;
- Establish minimum security standards for IoT-related devices in the global marketplace;
- Promote policies and practices that support better sharing of information about cyber attacks; and,
- Craft standards for protecting people's digital identities and even empower citizens themselves as active participants in that process.

5.1.4 Citizen autonomy with personal data

More than ever, citizens want to feel they have ownership of their personal data. Governments must, in simple terms, describe the often-complex processes involved in cyber security. This will maximise citizen autonomy for decisions around their personal data. Key messaging on the value of personal data collection, how the information will be used and what to expect next will be crucial.[2] This may mean working with industry to provide subject matter experts for public awareness campaigns.

Exploring technologies like digital identification and zero knowledge transactions to assure citizens that personal data is not stored by government will also provide a degree of confidence in the government's use of personal data.

5.1.5 Education campaign

Government has played the role of public educator in many different instances, particularly around the domains of national security and public health threats. Adopting a similar campaign approach to target risky behaviours and actions would have the double effect of educating individuals about the courses of action but would also signal to the public both the importance of this threat on the government's agenda and the expertise it possesses to combat that threat.

5.1.6 Communications approach

Citizens globally are calling for more dialogue with government.[3] Communicating with citizens about how and why their information will be used and how it can benefit them, will be key to establishing a positive dialogue with citizens about cyber security.[2] If citizens understand why certain procedures occur and grasp how they will benefit from them i.e. "reduce risk of cyber attacks," then their willingness to engage with government on this topic will increase. It may also be key to maximise two-way communication by using social engagement platforms to provide avenues for citizens to have their say. Cyber security is confusing and can be scary for citizens, so it is important for government to acknowledge this and engage with them about their concerns.

5.2 First response is essential

Every time the government handles citizens' concerns well, it builds and reaffirms government-citizen trust.[2] The converse is also true, when governments fail to adequately protect citizens and fail to respond to cyber incidents, citizens feel exposed and public trust is eroded. The Australian Government needs to be seen to be proactive and then transparent when there are issues relating to Australian cyber security.

References for Q5

1 Building citizen trust above and below ground, 2019, Accenture. https://www.accenture.com/us-en/insights/us-federal-government/cyber-resilience-building-citizen-trust

2 Trust: The Foundation For Service Citizens In a Digital World, 2017, Accenture. https://www.accenture.com/_acnmedia/pdf-69/accenture-citizen-trust-pov.pdf

3 Americans and Cybersecurity, October 2017, Pew Research Center Americans and Cybersecurity, 2017, Pew Research Center. https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity

4 Securing The Digital Economy: Reinventing The Internet for Trust, 2019, Accenture https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

5 Centre for Cybersecurity, World Economic Forum. https://www.weforum.org/centre-for-cybersecurity

6 Singapore's Operational Technology Cybersecurity Masterplan, 2019, Cyber Security Agency of Singapore. https://www.csa.gov.sg/~/media/csa/documents/publications/ot_masterplan/otcybersecuritymasterplan.pdf

7 The Economic Impacts of Inadequate Infrastructure for Software Testing Final, 2002, U.S Department of Commerce. https://www.nist.gov/sites/default/files/documents/director/planning/report02-3.pdf

8 New guidelines for responding to cyber attacks don't go far enough, December 17, 2016, Adam Henry & Greg Austin. https://theconversation.com/new-guidelines-for-responding-to-cyber-attacks-dont-go-far-enough-108908

Q8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

There is a growing volume of offerings that aim to increase cyber security for organisations. Determining the most sensible approach will require organisations to reflect on their current cyber risk profile and maturity. The following cover Accenture's view of important and sensible approaches to increase the cyber security maturity of industry or government.

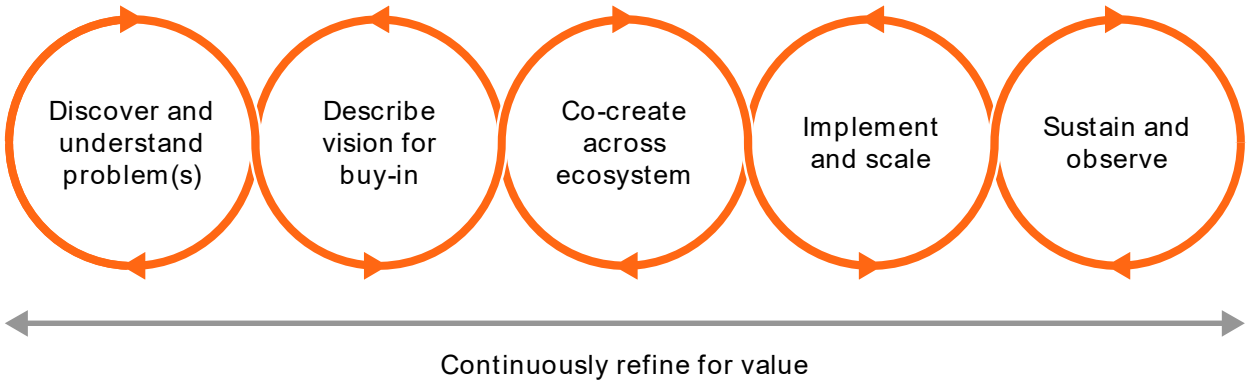
8.1 Increase strategic cyber maturity

Business and government need to adopt an agile form of strategy to combat the evolving nature of cyber security. A strategic feedback loop is required to ensure governments are both proactively and reactively responding to cyber risk.[3] Accenture recommends an iterative approach to strategy following the principles of systems, agile and design thinking. Figure 4 demonstrates Accenture's proprietary approach to strategic agility.

8.1.1 Build threat intelligence capability

Accenture understands that the Australian Government already has a matured threat intelligence capability which has been bolstered through the establishment of the Australian Cyber Security Centre. Many large private enterprises have built similar capabilities. Accenture has worked with several corporate customers in Australia to develop new capabilities using curated open source intelligence (OSINT), collated with internal and external telemetry to provide actionable threat intelligence that is specific to their environment.

Figure 4: Accenture's proprietary approach to strategic agility



8.1.2 Decentralising security capability

Accenture 2018 research '*Build pervasive cyber resilience now: securing the future enterprise today*' has found that 74 per cent of organisations have cyber security as a centralised function.[14] Contradicting this, a similar percentage of organisational executives believe that security staff and activities need to be decentralised throughout the organisation to maximise cyber security efficacy.[3] Building cyber security capabilities across all members of a workforce is key to increasing the effectiveness of cyber security. Extending this, maximising the cyber security capability of Australians will then naturally improve national cyber security. To promote cyber security capability, government and industry should look across workforce planning strategies to link technology, processes and people holistically.[11]

8.1.3 The nexus of Security Operations Centres

A Security Operations Centre (SOC) is a structural entity that combines cyber and physical security to provide better proactive cyber management for operational technology. The SOC breaks down the silos between physical operations and security technologists thereby improving communication and situational awareness. Working together operations and security staff can map the digital connectedness and cyber risk profile of each operational asset. Understanding these risk profiles leads to increased cyber vigilance.[12] In addition, a SOC provides a structure to house monitoring and analytics capabilities that are fully integrated into asset operations.

Establishing a SOC would not replace existing risk management strategies at executive and board levels in an organisation. It alternatively provides a two-stream approach to cyber risk integration, accelerating an organisations cyber security effectiveness.

8.1.4 Develop a safety culture across government and industry

If employees believe that their organisation is protected by technology that guards against data breaches, they will become less vigilant and exhibit riskier behaviour.[11] Empowering employees by clearly assigning them responsibility for how their behaviour contributes to the overall cyber security of the organisation is key. To do this, leaders across government and industry are advised to:[3]

- Be clear on the purpose of cyber security. Explain why taking precautions and being vigilant against cyber threats is important. Address how they relate to cultural safety more widely;
- Champion pragmatic behaviour change without restraining flexibility. For example, discouraging employees from writing down passwords and keeping them close to computers;
- Develop a security curriculum that's customised to individuals' specific roles. This will maximise individuals' autonomy and therefore responsibility;
- Promote healthy scepticism by adding security drills to routine operations;
- Use simulations to provide individuals first-hand experience of a cyber attack such as a moral phishing simulation; and,
- Identify and reward individuals and organisations 'doing the right thing.'

8.2 Increase technical cyber maturity

The foundation of technical cyber maturity lies in it being a consideration at the outset. Technical designs or architecture that do not include consideration to cyber security from inception need to be considered incomplete or impractical. Outlined below are key leavers for increasing technical cyber maturity.

8.2.1 Embracing DevSecOps

DevSecOps is an approach to technology development that allows for the continual iteration of code to ensure quality in design and output. Without proper design, technology products built to enable better data capture and sharing can introduce a significant amount of risk. Forrester research from 2019 has shown that addressing security early in the development lifecycle is 30 times cheaper than doing so in production.[13]

Many IT development lifecycles across industry and government rely on waterfall development. This usually means that high-level security approaches are developed up front and only reviewed by a cyber security officer after the development is complete. A more effective way of tackling cyber security in government is to integrate security team members into DevOps teams allowing for iterative and continuous improvements to security transparently and in real-time. DevSecOps approaches give developers the early feedback they need to be better stewards of good code and ensure government infrastructure has security baked into it from the moment it is developed.

8.2.2 Software-defined networking

Government and industry need to think about new ways to approach data transactions and information sharing. Software-defined networking (SDN) is a configurable network architecture that automates security provisioning and makes network pathways harder to find and attack.[9] By using SDN an agency will be able to use intent-based networking approaches which add additional context, learning and assurance capabilities.[9] Unlike internet-based networking, SDN assures its users of the intent of the collaboration and reduces the time to restore network functionality if an attack occurs.

8.2.3 Network enclaves

Network enclaves are an architectural way to create environments that allow better monitoring of users and applications sourcing an organisation's data. Access to a data enclave is controlled by the guardian of that enclave, and only known actors are able to enter, this creates a secure environment. An enclave can contain mainframes, application and database servers connected to network gateways that are protected by PKI certificate authority and registration authorities and network infrastructure components (domain name and time servers). Enclaves are underpinned by directories and "domain controllers" through approved intranet web servers and managed network components and/or internet proxy servers. All components are shared within the users of the enclave and are highly securable.[4]

8.2.4 Cloud as a cyber security strategy

Traditionally governments, particularly agencies dealing with intelligence, shy away from cloud and cloud technologies. But with the evolution of cloud offerings we are seeing cloud technologies that harness the ability of elastic workloads, multizone computing, and multi-cloud strategies to fend off adversaries. These aspects of cloud evolution mean that the cyber risks associated with cloud computing are becoming on par or below that created by local networks.[8]

Cloud security is set to evolve quickly with multi-cloud approaches growing. For example, the Banking sector is beginning to maximise the use of multi-cloud technology after the Australian Prudential Regulation Authority (APRA) updated its regulations and guidelines for use of cloud services.[15]

8.2.5 Security automation

There is a growing array of Security Automation and Orchestration tools (SAOs). These tools apply machine learning approaches to search, detect and act at speeds faster than any security analyst can accomplish.[2] These technologies will not replace security analysts but will harden organisations to cyber attacks through constant and mechanised vigilance.

8.2.6 Monitor

Continuous monitoring of cyber threats to software, firmware and hardware can enable organisations to be proactive and aware of the cyber threat landscape.[3] Monitoring throughout development can detect high-risk vulnerabilities in systems early and integrate security into the development cycle. Monitoring anomalous and suspicious human activity such as unauthorised access attempts, password failure rates and suspicious user behaviour will also provide proactive information on the likelihood of a cyber threat.

8.2.7 Patch systems – simple and effective

The simplest—and one of the most effective—strategies for increasing the security of a system is to patch it. For all systems, it is wise to introduce automatic notifications to users when applications require a patch and place enforced timers on the notification to make sure patches are applied in a timely manner.

8.3 Platform approach

Historically, organisations have attempted to load all information from all sources into a bespoke technical solution. This ultra-customisation for a specific service is no longer economical and provides limited security advantage. Continuing to pursue siloed customisation will result in organisations defraying costs and failing to proactively manage new and emerging threats.

A platform approach offers the advantage of integrating and connecting the flow of digital information through an ecosystem of providers. Pooling the digital information enables proactive identification and sharing of cyber risks across all actors on the platform. It is also economically favourable, with reduced ongoing costs for organisations using the platform.

8.3.1 Tiered approach to data protection

Due to the payoff between security and flexibility in regard to data use, a tiered approach to data asset management is a sensible approach for both government and industry to enhance cyber security. Organisations can identify and organise their data sets in order of risk and value. Questions such as, 'How catastrophic is the impact if this data were published on the front page of the newspaper?' are a good way to determine the value of data. Strategically investing in security measures that harden high-value assets as a priority can then increase cyber security in a sustainable way.

8.3.2 Digital identity-as-a-platform

The adoption of a shared and re-usable digital identity which can be used as a credential for secure services is rapidly becoming a reality. The more a digital identity is used the 'stronger' it becomes, as there is a known history from the time the digital identity is first registered. This history offers secure service providers assurance of the authenticity of the individual using the identify and therefore the trust level for that identity.

Looking across the domains of secure travel, financial services and security vetting, a digital identity platform can significantly reduce the need for time-consuming in-person authentication and support a near-seamless process for individual's identity verification. In addition, a digital identity platform provides small businesses including 'mum and dad e-commence stores' a way to securely manage their customers. Instead of creating their own secure identity process, or not having one at all, small businesses can leverage a platform that becomes stronger and more protected every time an identity is validated and a service is added.

While digital identities will increase the effectiveness of digital offerings, the introduction of a digital identity can create another lucrative target for threat actors. The required controls to avoid digital identities becoming the subject of cyber fraud will include a response approach to digital identity breach with a plan for isolation, controlling and notifying the impacted individual.

8.3.3 Authentication

Moving to a platform approach means it is important to limit, monitor and segment access to data platforms. The first approach is to use appropriate role-based controls to identify user groups and determine the minimum access requirements to fulfil those user groups' business role. Most platform offerings will have user roles and their privileges configurable to save organisations' effort and investment.

Use of two-factor authentication automated decisions about who can see which data and systems will also enhance the authentication process. While most two-factor authentication relies on the use of email or SMS, there are increasing incidences where threat actors have leveraged weaknesses in the phone network to get access to the code. Other options include use of a secure authenticator application such as Symantec or Google Authenticator.

As discussed above, digital identify could also be used as a common credential for the purpose of authentication into systems both physically and digitally. Using a digital identity would remove the need for username and password combinations for digital systems and the need for access cards for physical systems. Following on from the Digital Transformation Agency's shift to a common set of policies, procedures and exchange through the Trusted Digital Identify Framework (TDIF), more organisations will adopt digital identities to improve the efficacy and security of their digital and physical offerings.

8.3.4 Managing risk as-a-platform for global security intelligence

Managing cyber risk involves the assessment of devices, identities and the relationships between digital actors. There are a number of platform-based offerings that provide holistic cyber risk management by aggregating, curating and providing risk indicators to all users of the platform. The advantage of a platform approach to risk is that it can go beyond determining the risk of a single device or identity and instead highlight networks of risk.

Case studies – risk management as-a-platform

Microsoft Intelligent Security Graph – utilising telemetry techniques including collection of data from remote systems, Microsoft has developed an installable software that collects global information on things like trojans, viruses, email access, geographic locations to support device risk assessment. Users of the platform gain unique insights through a secure gateway.[7]

ThreatMetrix – a platform approach to digital identify risk management leveraging publicly available global shared intelligence. LexisNexis Risk Solutions has developed a platform that takes anonymised digital data related to a digital identity and its digital footprint to assess the risk based on previous interactions. Users of the platform are provided with a risk visualisation that displays the risk of an individual and their digital behaviour.[8]

References for Q8

[1] Securing the Digital Economy, Reinventing the Internet for Trust, 2019, Accenture. https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust-infographic-au.pdf

[2] Achieving Data Centric Security, 2019, Accenture. https://www.accenture.com/us-en/insight-data-achieving-centric-security-2017

[3] iDefense Cyber Threatscape report, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

[4] Enclaves: The Enterprise as an Extranet, 2000, Bryan Koch. http://www.ittoday.info/AIMS/DSM/82-10-83.pdf

[5] Recommendation of the Council on Digital Government Strategies, 2014, OECD. http://www.oecd.org/gov/digital-government/recommendation-digital-government-strategies.pdf

[6] Centre for Cybersecurity, World Economic Forum. https://www.weforum.org/centre-for-cybersecurity

[7] Advanced Security with Intelligent Security Graph, Microsoft. https://www.microsoft.com/en-au/security/operations/intelligence

[8] Threatmetrix Digital Identify Network, LexisNexis Risk Solutions. https://www.threatmetrix.com

[9] Software-Defined Networking, CISCO. https://www.cisco.com/c/en_au/solutions/software-defined-networking/overview.html

[10] 2019 Will be the year of cloud-based cybersecurity analytics/operations, 2019, Jon Olstik. https://www.csoonline.com/article/3331280/2019-will-be-the-year-of-cloud-based-cybersecurity-analyticsoperations.html

[11] Secure us to Secure me, 2019, Accenture https://www.accenture.com/gb-en/insights/technology/cybersecurity-digital-ecosystem

[12] Outsmarting Grid Security Threats, 2017, Accenture. https://www.accenture.com/t00010101t000000z__w__/gb-en/_acnmedia/pdf-62/accenture-outsmarting-grid-security-threats-pov.pdf

[13] The State of Network Security: 2018 to 2019, 2019, Forrester. https://www.forrester.com/report/the+state+of+network+security+2018+to+2019/-/e-res142234

[14] Build pervasive cyber resilience now: securing the future enterprise today, 2018, Accenture. https://www.accenture.com/_acnmedia/pdf-81/accenture-build-pervasive-cyber-resilience-now-landscape.pdf

[15] Information Paper: Outsourcing involving cloud computing services, 2018, APRA. https://www.apra.gov.au/sites/default/files/information_paper_-_outsourcing_involving_cloud_computing_services.pdf

Q9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

Accenture research estimates that the revenue opportunity at risk for Australian private industry in relation to cyber security exposure is 2.8 per cent annually over the next 5 years. This equates to a potential opportunity loss of up to $US5.2 trillion over the next 5 years.[1] In addition, our research shows that Australian's business leaders have the influence needed to collaboratively address cyber security issues.[2]

Engaging the private sector in the context of cyber security management is not about the government devolving its functions to the private sector, but rather about finding the right constructs or models to collaborate for the cyber security agenda.

9.1 Strategic capability

One of the main challenges for the Government will be sourcing and maintaining skilled security cyber professionals.[3] Historically, governments have relied on contractor or consulting models to fulfil specific capability needs, rather than developing internal specialist skills. Accenture 2016 research found that half of public service leaders globally (51 per cent) say their agencies mainly look to hire talent from the private sector when developing intelligent technology projects.[4] Governments will need to strategically engage with the private sector in order to leverage specialist cyber security skills. Below are some models to explore.

9.1.1 The capability retainer

Rather than cultivating in-house talent governments may seek to find providers that possess specialist capabilities and create a 'retainer' style contract. This will ensure the availability of resources at critical times without needing to recruit, retain and fund highly sought-after market capabilities. A retainer approach is particularly useful for cyber skills that are required ad-hoc, such as adversarial simulation and crisis response.

9.1.2 Trusted capability partners

One of the growing risks of cyber security is insider threat: the risks that current or past employees with access to critical cyber security information may pose a malicious threat. A model similar to the Department of Home Affairs' 'Trusted Trader' may be a useful paradigm to consider. Through a process of government vetting, businesses and individuals could become accredited as a trusted capability partner. Critical pieces of government work requiring specialised capability could then be devolved to private sector partners with confidence.

9.2 Decisions with data

Legal or executive decision lies with government. However, there are aspects of the data supply chain that can be devolved to the private sector. Private entities could easily collect, consider and analyse data to support a decision by government. This can be applied to platform-based approaches of data collection and management. The private sector holds much of the analytical expertise to make data work for government and industry in a secure way.

Intelligence-led policy design is another area where upstream activates that lead to government decisions could be devolved to the private sector. Developing machine learning algorithms to simulate and predict outcomes to proposed policy could be delegated to the private sector. However, clear and appropriate oversight from government ensuring they maintain ultimate decisions would be needed for public trust.

9.3 Citizen segmentation

Governments across the world are starting to understand the potential impact of data-driven citizen segmentation. Using this approach at the initial stages of policy and regulation development amplifies the impact on future citizen behaviour. Professional services organisations and industry more widely have been developing and applying customer segmentation approaches for decades. It therefore makes sense that governments could make use of customer segmentation capabilities from the private sector without investing significantly to build this internal capability.

Case study

Accenture provided citizen segmentation services to a compliance focused Australian government agency with the aim of improving rates of business compliance with Australian Government policy. By segmenting businesses into groups with similar characteristics and devising tailored treatments for each section the rate of compliance was significantly increased. This approach, while targeted at business in this case study, remains valid for citizens.

9.4 Platform approach

Devolving the creation and management of digital platforms to service provider(s) can be key to leveraging the capability of the market in relation to cyber risk. This would provide the best protection for both government and private sector without creating a single honey pot for exposure. Government will have assurance that platforms are built with consideration to security requirements by using trusted capability partnership models.

9.5 Public- private partnerships to make the most of new technology

Keeping up with the decreasing lifespan of ICT products and systems is an expensive and time consuming practice for governments. New and innovative partnership models with shared expense and therefore shared risk will be key for governments to provide the best and most up-to-date ICT services for Australian citizens. Sharing expense with the private sector will also decrease the risk of investing taxpayer dollars to novel and cutting-edge projects while at the same time ensuring the outcome of projects are in the public interest.

References for Q9

1 Securing the Digital Economy, Reinventing the Internet for Trust, 2019, Accenture. https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust-infographic-au.pdf

2 Reinventing The Internet Digital Economy, 2018, Accenture. https://www.accenture.com/au-en/insights/cybersecurity/reinventing-the-internet-digital-economy

3 Filling Cyber-Security Jobs in Government Is Vital, 2017, Accenture. https://www.accenture.com/_acnmedia/pdf-60/accenture-filling-cybersecurity-jobs-government-.pdf

4 Smart Move: Intelligent technologies make their mark on public service, 2016, Accenture. https://www.accenture.com/t00010101t000000__w__/gb-en/_acnmedia/pdf-29/accenture-public-service-intelligent-technologies-research–slideshare.pdf

Q11. What specific market incentives or regulatory changes should Government consider?

Determining effective market incentives or regulatory changes to improve Australia's cyber security posture will involve the Australian Government's collaboration with industry and the wider ecosystem. Accenture's proposed "Cyber Council" approach, outlined in Question 3, provides a structure for such collaboration. Accenture's approach to intelligence-led policy design is also relevant for the Australian Government as it aims to determine the most impactful and economical approaches for incentive and regulation. Despite the focus on collaboration and intelligence-led design, this section will outline some proposed initiatives for the Australian Government's consideration.

11.1 For the citizen

11.1.1 Cyber security initiatives/ key training on platforms such as myGov

With more Australians interacting with government services through myGov, this is an ideal platform to deliver cyber security initiatives for Australian citizens. Explanations during the login process that include the importance of a strong password and the benefits of multi-factor authentication would be an engaging way to deliver critical cyber security education to citizens. Timely information about the importance of verifying senders and highlighting known phishing campaigns through the platform would also enhance citizen awareness of cyber security.

11.1.2 Gamification of resources on cyber security/ information security

There is a significant amount of information for citizens provided by the Australian Cyber Security Centre through staysmartonline.gov.au. While the information on these sites is useful, it is presented as plain text and links, and may not be easily retained by users. Current thinking in digital learning is to create 'bite-sized' and 'interactive' modules to convey learning objectives. Turning these information sources into interactive learning sites through gamification would incentivise citizens to return to the site. Additionally, schools and education institutions could leverage the resources for their own learning approaches.

11.1.3 Vulnerable populations

As outlined in Question 1 some specific populations are most vulnerable to cyber attack. These are the ageing population, adolescents and young adults and citizens living with intellectual disabilities. There are physical places where these citizens most vulnerable to cyber attack attend including educational institutions, libraries and hospitals/health facilities. Free and targeted cyber security training and resources at these locations will boost awareness and safety in these most vulnerable populations.

Voting centres are also important places to spread cyber security training and awareness. As disinformation threats often increase around political events such as elections, voters have a significant need for increased awareness. Interventions here could be focused on, but not limited to, helping voters know the difference between credible and non-credible information sources.

11.2 For small businesses

11.2.1 Cyber security training and awareness for small businesses

Small businesses would benefit from government support for cyber security training and awareness initiatives. The cost of developing training internally for many small businesses is prohibitive and partly explains why less than 35 per cent of small business staff undergo cyber security training.[1] Providing cyber security training options both online and face to face for small business will fill the large cyber educational gap. Training may be offered either through the Australian Cyber Security Centre or through trusted providers. Government may consider subsidising the cost of the training to incentivise business uptake.

11.2.2 Alliance purchasing for small business

Government should assist small businesses utilise the most cyber secure vendors for their business processes. A potential way to do this would be for government to create a trusted vendor list and then partner with those vendors to provide small businesses technology offerings. That would allow small business to purchase in an 'alliance', making cyber security technologies more cost-efficient for individual businesses. Through the proposed "Cyber Council" the Australian Government can also lead discussions with industry partners, who can either act as or utilise their own ecosystems and networks in order to best match the cyber security needs of small businesses with the most appropriate vendors.

11.3 For enterprises

11.3.1 Supply chain incentives

Incentivising large enterprises to help bolster the cyber security capabilities of small businesses in their supply chain provides a benefit to all. Government could explore incentives through tax deductions or subsidies for enterprises who support small business within their supply chain.

This initiative could also work in tandem with the current Cyber Security Small Business Program, which provides a grant of up to $2100 for a certified small business cyber security health check.[2] Once the check has determined the areas that need attention, these small businesses can then work with larger enterprises in their supply chain. For small business without enterprise partners government could facilitate a 'buddy' system pairing small businesses with professional organisations.

11.3.2 Subsidies or tax deductions for proactive cyber security investments

Private entities play a key role in the cyber security landscape, and strategically incentivising proactive cyber security activities such as monitoring capabilities and adversarial simulations could be a key way to raise collective security. As well as increasing cyber defence capabilities, this also fosters enterprise collaboration and information sharing. Consideration of focused incentives to organisations supporting critical systems in Australia could also be strategically valuable.

11.3.3 Shared service incentives

Due to the demand for cyber security professionals, government incentives for organisations to share their capabilities with the ecosystem are worth considering. A shared service framework where cyber security professionals are consolidated across organisations or entities into a single service, whose mission is to provide cyber security services as efficiently and effectively as possible, could be key to solving the shortage of security professionals in the Australian market.[3] This is discussed further in Question 14.

References for Q11

[1] Data Breach Investigations Report, Summary of Findings, 2019, Verizon. https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings

[2] Cyber Security Small Business Program, 2019, business.gov.au.seen 21 October 2019, Australian Governement. https://www.business.gov.au/assistance/cyber-security-small-business-program

[3] High Performance Outcomes: Government Shared services, 2013, Accenture Federal Services. https://www.accenture.com/t20160803t233233__w__/us-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_22/accenture-high-performance-outcomes-government-shared-services.pdf

Q13. How could we approach instilling better trust in ICT supply chains?

As organisations and governments cannot easily control the security measures taken by all members of a given supply chain, one weak link could cause disruption to the entire chain.[2] To provide context to this response, Accenture has interpreted 'we' to mean government, industry and any organisation involved in supply chain management. And that 'trust in ICT supply chains' refers to assurance of the origin, quality and security of an ICT product coming to Australia.

13.1 Trust blockers

One laptop requires many hundreds of different materials to be sourced from across 18 countries.[1] The high complexity of this supply chain means that to secure it, assurance processes will be needed across many interactions traversing many jurisdictions. Below outlines some of the key contributors to the current blockers to establishing trust in ICT supply chains.

13.1.1 Who built it?

ICT supply chains are increasingly opaque as products built by one company are often re-branded and sold on as a product from a different company. Most consumers will not realise that their online purchase from an American company will have Chinese rebranded products sold on it. And the implications for smart products with software built internationally is that they are possibly tainted with the national interest of that company and can introduce cyberespionage risk.[4]

13.1.2 The efficiency paradigm and the role of the consumer

Recent Accenture research has found that 76 per cent of executives see the top-two customer demands for the future of supply chains as: "more customised products and services" and "faster order fulfillment times."[3] These customer demands increase pressure on supply chains to be as fast and efficient as possible. However, as more products and services are introduced to supply chains the number of transactions increases, as does the complexity of security measures required. Educating consumers to demand safe transactions is essential to justify the trade-off between security and efficiency in supply chain management.

13.1.3 The cost of increasing security

Developing economies are often the cheapest suppliers of ICT equipment, but they also represent some of the highest cyber security risks. If governments intervened to block or ban suppliers with known affiliations, there will be cost implications that citizens and small businesses may need to absorb.

13.1.4 Lack of visibility

ICT manufacturers and distributors struggle to understand whether they meet customer expectations because they lack visibility of orders, inventory and delivery vehicles.[4] This lack of visibility has significant security implications. Australian's can't build trust in their ICT if they have no visibility of where their product is being sourced from our how it is getting to them.

13.2 Trust builders

Building trust in ICT supply chains is complex and requires consideration of many factors before intervention(s) can be made. Given that Australia has very little onshore ICT manufacturing, building trust in ICT supply chains will need to be managed globally and in concert with supply chain organisations.

13.2.1 Better management from supply chain organisations

John Lindquist, chief executive officer of EWA Information and Infrastructure Technologies, observed that "trust should not be based where the headquarters is located."[1] Lindquist has identified that most organisations involved in supply chain management are global in nature and that to increase trust in supply chains' cyber security issues must be considered and managed as a global issue. Accenture recommends the following to better manage global supply chains for trust:

- **The 'Supply Chain Architects.'** People in this role will become responsible for configuring multiple unique supply chains that are 'quarantined' for security. Their role will include networking through partnerships and platform-based approaches to tailor specialised supply chains to maximise both their security and efficiency.[3]
- **Platform approach, not asset approach.** Moving supply chain players to collaborate on a single platform that is available globally will increase the visibility of transactions and increase the data available to collaborators on that platform.[4]
- **Align supply chain risk management strategy with cyber security strategy.** Include cyber strategy as a core function of the global organisation considering the best technology options.[6]

13.2.2 Government research and development

Accenture's view is that that the future supply chain will need to be self-learning, self-correcting and insight-driven.[3] This will require organisations and governments adopting emerging technologies and investing in research and development (R&D) in this area. An area of focus for government R&D should be intelligence-driven supply chains, that is, supply chain technology that uses artificial intelligence, machine learning and other techniques to improve the interactions between people and machines, maximizing overall productivity and enabling automated security measures.[3]

13.2.3 Intelligence-driven supply chains

It is essential for building trust that organisations managing supply chains are capturing the right data, and also using it in the right way. The application of analytics software can assist in 'what-if' scenario modelling. Continuous monitoring of visually displayed metrics can provide early indication of the health and function of a given supply chain. This can enhance the assurance Australians have of the ICT products arriving in Australia.

13.2.4 Global regulation

Cyber security regulation that traverses geographies will unify the defence of a supply chain and harden it to attacks. This regulation would include a set of common, minimum and mandatory standards that apply to all entities in a given supply chain no matter their location. An added benefit of introducing an international legal standard is that it increases trust between nations and facilitates information sharing.

13.3 Mandating a standard for critical systems supply chains

Until recently, managing the security of supply chain partners was not considered an essential action for organisations and governments managing critical systems. But, as threats from cyber increases, establishing a responsible entity in the supply chain and determining their responsibility to manage the cyber security of their vendors should become the standard and be enforceable by government.[2] This approach should be considered a "win-win" approach for the responsible entity, as it can help to protect all supply chain parties from cyber attacks and strengthen already-established links.

Case study

To safeguard North America's electricity supply, the North American Electric Reliability Corporation (NERC) has issued several critical infrastructure protection (CIP) standards. The proposed CIP-013-1 standard (subject to Federal Energy Regulatory Commission's approval) addresses the vulnerabilities and threat vectors that external third parties in the supply chain can have on the Bulk Electric System (BES). It helps to mitigate the risks of supply chain cyber security incidents that affect BES reliability, and requires responsible entities, which can include utilities and a wide variety of other stakeholders, to develop plans, policies and procedures concerning their supply chain vendors.[5]

13.4 The role of blockchain

Blockchain is now high on the agenda of most leading customs and trade organisations.[6] And while blockchain does have great potential to enhance the visibility of supply chains, Accenture does not believe it provides the 'silver bullet' for managing trust in supply chains. It is most important to consider the right technology used in the right way. Organisations should consider blockchain as part of a toolbox to increasing trust in supply chains.

13.5 Lessons from modern slavery and supply chains

A use case for the Australian Government to reflect on is the approach to addressing modern slavery in supply chains. The way the Australian Government has engaged the providers and public on this issue has already achieved significant gains in increasing trust in supply chains around modern slavery. Lessons from this approach will be useful when the Australian Government seeks to address trust in ICT supply chains.

Case study – supply chain traceability using blockchain in the food sector

The Gordon and Betty Moore Foundation commissioned Accenture to undertake a study exploring the feasibility of blockchain to enable end-to-end supply chain traceability in the food sector. The study looks at the opportunities and challenges of implementing this emerging technology, including business benefits and governance considerations. Relevant outcomes of this study showed:[7]

- Blockchain makes it possible for a system of independent actors to share and trust a record of digital assets, transactions, and information. However, blockchain should be evaluated against other technologies with a specific use case to quantify benefits and costs.
- To implement a blockchain traceability system, the digital maturity of supply chain partners may need to be addressed. That could mean a significant amount of up-front cost required from across supply chain partners may impede the progress required to achieve sufficient integration and interfacing.
- Private, public, and hybrid blockchain solutions each have unique strengths and weaknesses depending on specific requirements. It is not necessary to build applications on a public blockchain to reap the benefits of transparency and accountability.
- There is a vital role for regulators to take a lead in the adoption of blockchain traceability solutions and multi-stakeholder collaboration.

References for Q13

[1] Twelve Ways to Build Trust in the ICT Global Supply Chain, 20 1320 16, Brookings Institute. https://www.brookings.edu/wp-content/uploads/20 16/06/ 18-global-supply-chain-west.pdf

[2] Supply Chain, the weakest link in cybersecurity, 20 19, Australian Cybersecurity Magazine. https://australiancybersecuritymagazine.com.au/supply-chain-the-weakest-link-in-cybersecurity

[3] Architecting the 2025 Supply Chain, 20 17, Accenture. https://www.accenture.com/_acnmedia/pdf-66/accenture-future-supply-chain-pov-final.pdf

[4] Is Your Supply Chain Holding Growth Hostage? 20 18, Accenture. https://www.accenture.com/_acnmedia/pdf-81/accenture-intelligent-supply-chain-consulting-pov.pdf

[5] Forging Stronger Links, NERC CIP Supply Chain Cyber Security, 20 18, Accenture. https://www.accenture.com/_acnmedia/pdf-88/accenture-nerccip-suppychain.pdf

[6] Blockchain: Mapping new trade routes to trust, 20 18, Accenture. https://www.accenture.com/gb-en/insights/public-service/blockchain-trust-mapping-new-trade-routes

[7] Tracing the Supply Chain: How Blockchain can enable traceability in the food industry, 20 18, Accenture. https://www.accenture.com/_acnmedia/pdf-93/accenture-tracing-supply-chain-blockchain-study-pov.pdf

Q14. How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

Cyber security must become a core competency for all roles. However, the need for specialised skills will also be paramount. Observations from recruitment business Hays' security skills research indicate that the demand for cyber security professionals outstrips the available capability. Data collected from business leaders across Australian and New Zealand show that 61 per cent find it difficult to very difficult to recruit and retain cyber security talent.[1]

The next-generation of Chief Information Security Officers' (CISO) roles will need to be expanded from their predecessors and extend beyond information security, aligning with the business, and leading it in the cyber security strategy for technology, ecosystems and the overall operating environment. To achieve this, individual CISOs must be agile, support business objectives, and understand the broader scope of security including connected products, smart services, and supplier and distribution ecosystems to demonstrate the art of the possible to the CTO or CIO.[2]

Building and maintaining the numbers required in the cyber security workforce will be a hurdle for the Australian Government and private entities.

14.1 New capability model based on shared services

The scale of the demand for cyber professionals in Australia will require novel ways of staffing to make the most of the available capability in the market. Instead of individual organisations building and maintaining internal talent, a shared services approach may be an optimal model. Shared services are the consolidation of specialist support functions, such as cyber security, from several organisations or entities into a single organisational entity whose mission is to provide services as efficiently and effectively as possible.[3] By leveraging a pool of cyber professionals across ecosystems of organisations we can begin to efficiently use those individuals with the required skills.

The establishment of a shared service model will require collaboration across government and industry. As introduced in Question 3, a 'Cyber Council' model to define the approach to consolidating cyber security offerings for Australia would be ideal. Consideration must be given to an approach to share intelligence and services in a way that does not stifle market competition and create competitive advantage. Possible approaches could be to provide incentives to companies that are willing to share services or people, or to leverage crowdsourcing techniques.

14.2 On the job training with industry

Where professional service organisations can support the effort of building cyber security professionals is through coaching and partnerships to upskill existing workforce members in real-world or 'on-the-job' experience. Such programs provide real-time and light-touch interventions that guide the development of staff on the job and improve capabilities without the need for time out for extended classroom or online training. On-the-job training is demonstrably more effective than classroom or online training.

Case study

A training program Accenture has employed involved a partnership with a government defence organisation to improve the capabilities of individuals to seed and grow innovation activities. By providing real-time feedback and applying skills in the 'on-the-job' context the results of the program exceeded expectations. Not only were staff skills measurably improved, the organisation has since allocated dedicated teams and additional budgets to complete in situ testing efforts, and the findings from the projects are being incorporated by the respective areas.

14.3 Addressing skills shortage – raise, train, sustain

High school curriculums for IT and computing have only just recently evolved to include the basics of coding, and curriculums are often slower to update than the rate of industry change. Students are not being exposed to real-world cyber security experiences early or often enough. To address this, the defence operational readiness framework of raise, train, sustain provides a useful structure to build cyber capability in Australia.

14.3.1 Raise

One approach is to consider a new discipline, 'security thinking', to be developed and implemented through all levels of education. Just as critical thinking is imperative to English, Media Studies, Information Technology and more, 'security thinking' could be another enhancement to the readiness of Australians to enter the workforce. Other interventions such as industry partnered special skills days for schools and universities can help identify and raise the next generation of cyber security professionals.

14.3.2 Train

Training and remaining up to date for cyber security is required in all organisations, no matter what their size. Accenture's view of the best way to train for cyber security is to undertake regular simulations with people to learn how they are primed for such a cyber security event.[4] Professional service firms are well placed to offer 'simulation-as-a-service' capabilities to help mature the cyber readiness of an organisation.

14.3.3 Sustain

Sharing information between organisations and building informal networks between CISOs and their peers and government collaborators will be a key aspect of sustaining these skills. Peer attitude and behaviour are key motivators for performance and keeping security professionals engaged will require opportunities for collaborations and lessons learnt.

14.4 Skilled migration

Partnering with industry to identify and bring cyber professionals to Australia for short or extended periods to help inject their capability and know-how will be key to establishing a highly-skilled cyber security workforce. The Australian Government may need to find migration schemes that target cyber security capabilities.

14.5 Cyber Council as an innovation incubator

The Cyber Council outlined throughout our response, could also act as a training and education enabler to help solve the cyber skills shortage in Australia. The Cyber Council could develop and provide specialised learning materials for schools and universities. This in turn can provide an incubation area for cyber security start-ups that are often drawn away from Australian shores to countries like the U.S.

References fo Q14

1 Cyber Security Talent Report Addressing the Skills Gap, 2019, Hays. https://www.hays.com.au/cs/groups/hays_common/@au/@content/documents/webassets/hays_2051431.pdf

2 Securing the Industrial Enterprise, 2019, Accenture. https://www.accenture.com/t20190313t174133z__w__/lv-en/_acnmedia/pdf-96/accenture-securing-the-industrial-enterprise-cyber-resilience.pdf

3 High Performance Outcomes: Government Shared services, 2013, Accenture Federal Services. https://www.accenture.com/t20160803t233233__w__/us-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/dualpub_22/accenture-high-performance-outcomes-government-shared-services.pdf

Q17. What changes can Government make to create a hostile environment for malicious cyber actors?

Accenture believes that the best defence is an effective offense. This starts with having a mindset of thinking like an attacker. By enhancing threat intelligence capabilities and employing advanced adversary simulation techniques government can create a hostile environment. Government should also collaborate with private sector organisations to establish relevant policies, frameworks and education to support the private sector in adopting a similar mindset.

17.1 Introducing the 'Cyber Ranger'

Detecting and counteracting the spread of deliberate disinformation can be difficult. Like a large national park, cyber space is large, complex and largely hard to visualise. A ranger's role is to manage a complex environment by regularly scanning for threats, conducting activities that improve the resilience of the environment against threats, as well as protecting and supporting vulnerable parts of the environment. These are key to the security management of cyber space. A new role that the Australian Government could consider is developing 'Cyber Rangers' to protect and sustain Australia's cyber environment.

Case study: the 'Baltic Elves'

In Estonia, a highly digitised country that suffered a massive cyber attack in 2007 and continual disinformation campaigns, volunteer 'Baltic Elves' monitor the internet for disinformation, a CyberDefense League of IT specialists shares threat information, and the government has fined or suspended biased media sources as a result of their work protecting Estonia's cyber space.[3] While in this example the 'Baltic Elves' are volunteer, there is significant value in exploring the role of a 'Cyber Ranger' as a professional capability.

17.2 Adversary simulation

Adversary operational simulation is a key activity to promote cyber resilience and hence create a hostile cyber space for threat actors.[1] Just as the military prepare for battle threats through operational simulations, government needs to be preparing for the inevitable cyber attack.

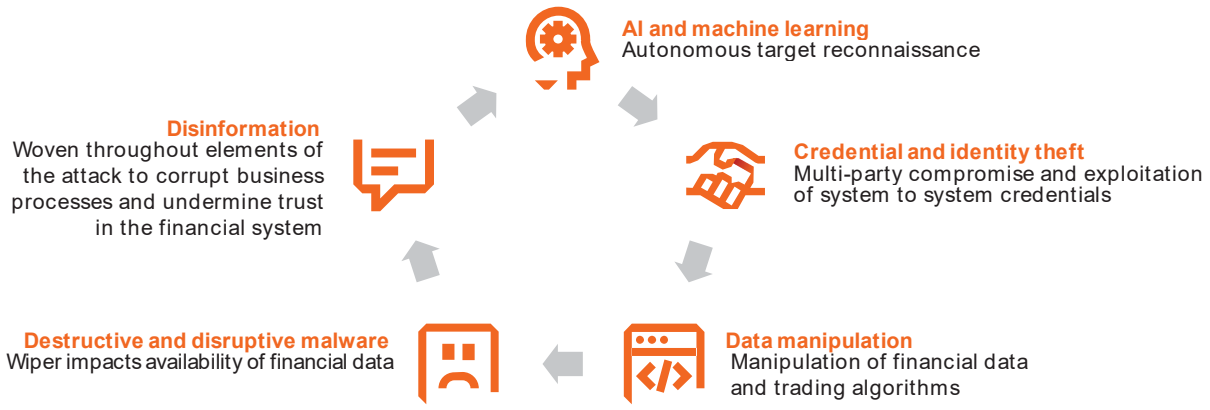
Adversary simulation is the collaboration between organisations on multistage exercises. They involve scenarios ranging from simulations of disinformation, adversary emerging technologies and compromised corporate credentials.[4] To ensure the simulation reflects the real-world threat landscape, it is important that these simulations occur 'against' a partner with the capabilities to break into an organisation's network, target a business process and leverage extensive threat intelligence.

Figure 5 below displays the plausible scenarios that can be simulated to increase a hostile environment for threat actors in the future.

Case study – simulation exercises with iDenfense Threat Intelligence

Accenture's Advanced Adversary Team combines industry-leading research with iDefense Threat Intelligence and deep cross-industry experience to simulate relevant threats for clients. Simulations help security operations teams prepare for worst-case scenarios and take cyber resilience to the next level of maturity and effectiveness. When the team partners with an organisation to undertake adversarial simulations, a realistic adversary and tailored objective is defined. For example, a specific type of malware may be used to test the organisation's ability to respond directly to that threat. At the end of the exercise, the organisation has personalised insights into the opportunities for improvements to that threat, preparing the organisation. The team develops a report with key findings and improvement suggestions for the client to deploy across its organisation, allowing clients to evaluate whether their security teams are properly tooled and resourced to defend against even the most sophisticated attackers.

Figure 5: Plausible scenarios for adversarial simulation



Source: Accenture iDefense Threat Intelligence

17.3 Invest in a citizen reporting mechanism with an education campaign

Identifying and reporting cyber threats early and at the most granular level will be key to creating a hostile environment for cyber threat actors. A 2018 study '*Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom*' reviewed data from over 500 citizens in the United Kingdom and found evidence that the majority are unsure about how to report a cybercrime event.[2] No such research has been conducted in Australia to date.

Even though the reporting process to the Australian Cyber Security Centre is simple, there is a necessity for citizen awareness of how and when to report. Clear and well communicated education campaigns from government will be needed to maximise citizen action in detecting cyber threats early.

As social engineering campaigns via email remain a top mechanism that threat actors employ, Accenture recommends a public education campaign that targets the below:[2]

- Education to help citizens recognise and avoid fraudulent e-mails;
- Guidance for citizens on how to identify and respond if they believe they are victim of a social engineering attack;
- A simple framework for citizen adoption of non-risky behaviour; and,
- Recommendations of security technology to use and how to keep this updated.

17.4 Attribution as a deterrent

The classical use of deterrents as offence techniques is hard to apply to cyber security. Joe Burton writes in '*Deterring cyber attacks: old problems, new solutions*' that a growing premise among security professionals is reconstructing the digital environment itself so that users must be identifiable and therefore attribution is clear.[6] This is something that will take a global community to devise and implement. Until then, improving the cyber resilience of people, organisations and governments will be key to creating a hostile environment for cyber threat actors.

17.5 Co-create industry standards for resilience and regulate

Each industry will have differing cyber threat profiles and thus require industry-tailored standards. Accenture recommends that industry standards are co-created with industry leaders through a "Cyber Council" approach as outlined in Question 3. Industries within Australia and globally are at different levels of maturity regarding cyber security. Below are two key examples demonstrating the need for an industry standard approach.

17.5.1 Example 1: Industrial equipment industry

2019 Accenture research found that 74 per cent of industrial equipment executives said that "cyber attacks are a bit of a black box, we do not quite know how or when they will affect our organisation."[4] Couple this with data that the number of cyber attacks on industrial equipment organisations is rising year over year with on average, 177 security attacks in the last year, with 17 per cent successful in breaching defences. This means that the industrial manufacturing industry needs support to identify the types of threats it is facing and how best to mitigate them.

17.5.2 Example 2: Electrical infrastructure

Accenture's 2017 Digitally Enabled Grid survey revealed that the cyber maturity of electrical critical systems has room to grow. Electricity distribution business executives cite interruptions to supply as their greatest cyber attack related concern, closely followed by potential impacts on customer and employee safety.[5] Electrical distribution grids span a wide range of digital automation, from SCADA-controlled sub-transmission down to passively-run, low-voltage residential feeders, making them vulnerable targets to cyber attacks.

Utilities are at varying stages along the cyber protection maturity curve. Some are merely working toward compliance with local security standards, while others have already achieved compliance and are working on developing security as a core business capability.[5]

References for Q17

1 Future Cyber Threats, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf

2 Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom, 2018, Lee Hadlington. https://www.cybercrimejournal.com/HadlingtonVol12Issue1IJCC2018.pdf

3 Managing Ransomware: Practical steps to avoid future attacks, 2017, Accenture. https://www.accenture.com/_acnmedia/pdf-58/accenture-security-ransomware.pdf

4 Securing the Industrial Enterprise: Achieving Cyber resilience in Industrial Equipment, 2019, Accenture. https://www.accenture.com/t20190313t174133z__w__/lv-en/_acnmedia/pdf-96/accenture-securing-the-industrial-enterprise-cyber-resilience.pdf

5 Outsmarting Grid Security Threats, 2017, Accenture. https://www.accenture.com/t00010101t000000z__w__/gb-en/_acnmedia/pdf-62/accenture-outsmarting-grid-security-threats-pov.pdf

6 Deterring cyber attacks: old problems, new solutions, 2018, John Keane. https://theconversation.com/deterring-cyber-attacks-old-problems-new-solutions-96279

Q18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

Accenture believes governments and private entities need to adopt a proactive and intelligence-led approach to identifying and remediating cyber threats, requiring a "think like an attacker" mindset. This is not a novel approach, war philosophers have been proponents of 'know your enemy' tactics for centuries.

> **"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."**
>
> – Sun Tzu[1]

Applying the same philosophy to cyber threats leads to four overarching cyber defence objectives:[2]

- **Know your threat** by using artificial intelligence (AI), machine learning (ML) and cyber threat intelligence to understand the threat landscape.
- **Be your threat** simulate threat using advanced adversarial techniques to simulate threats and understand how to respond to them.
- **See your threat** through threat hunting and active monitoring and detection capabilities.
- **Expel your threat** using on-demand incident response and recovery.

18.1 Know your threat

Government and private organisations need to shift from defending against known cyber threats to proactively seeking out new threats through applied cyber threat intelligence. Threat actors are increasing in their sophistication and patience, continually trying and inventing different techniques. Just like national security agencies study their adversaries to learn their techniques (and how to counter them), private organisations need to adopt a similar approach.[3]

Accenture's Advanced Adversary Team combines industry-leading research and development capabilities with iDefense Threat Intelligence and deep cross-industry experience to simulate relevant threats to help security operations teams prepare for worst-case scenarios and take cyber resilience to the next level of maturity and effectiveness.

Similarly, government can play an important role in aiding operators of critical private networks and systems to adopt a similar intelligence-led threat identification capability. This may range from sharing intelligence on emerging threats that are targeting particular industries, through to providing tools and "tradecraft" techniques to organisations to support their own threat intelligence gathering.

18.2 Be your threat

Like the military prepare for battle threats through operational simulations to iterate defence strategies and improve operational readiness, government and private entities need to be preparing for the inevitable cyber attack. Adversary simulation can range from separate red teams (attackers) and blue teams (defenders) challenging each other, through to collaboration between organisations in an industry-wide exercise. They involve scenarios ranging from simulations of disinformation, adversary emerging technologies and compromised corporate credentials. Importantly, they need to closely emulate the range of activities and techniques used by attackers, so it is important that these simulations are done with a partner with the capabilities to imitate what an attacker would do to reflect the real-world threat landscape.

18.3 See your threat

The ability to detect threats before they can cause damage is a key part of a proactive defence strategy. Using insights gained through threat intelligence, government and private organisations can hunt for the tell-tale signs that a compromise may have already happened. This process needs to go beyond just rules-based detection systems that detect "signatures" or IOCs (indicators of compromise) from known attacks. It requires capable individuals with understanding of the latest techniques that attackers use to bypass conventional detection mechanisms.

Continuous monitoring of cyber threats to software, firmware and hardware can enable organisations to be proactive and aware of the cyber threat landscape.[3] Monitoring throughout development can detect high-risk vulnerabilities in systems early and integrate security into the development cycle. Monitoring anomalous and suspicious human activity such as unauthorised access attempts, password failure rates and suspicious user behaviour will also provide proactive information on the likelihood of a cyber threat.

18.4 Expel your threat

Once a compromise is detected and understood, it needs to be contained and eventually expelled. There is much to gain from ongoing covert monitoring to understand the attacker's motivations and techniques. Eliminating the compromise too early, or too overtly, may result in altering attackers and sending them elsewhere. Using techniques such as network segmentation means compromised servers, devices and credentials can remain active, but with reduced connectivity, thereby containing downstream impacts.

References for Q18

[1] The art of war, Sun Tzu, available at https://suntzusaid.com

[2] Accenture Cyber Security Fusion Centre. https://www.accenture.com/au-en/service-accenture-cyber-fusion-center-washington-dchttps://www.accenture.com/au-en/blogs/blogs-cyber-defence-reactive-proactive

[3] Future Cyber Threats, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf

Q19. What private networks should be considered critical systems that need stronger cyber defences?

Accenture's view is that the Australian Government should consider critical systems as any system where an attack could have a material impact on national security, citizen safety, financial or economic impact to the nation or seek to materially disrupt Australian societal values. Accenture's view of critical targets for cyber attack that would lead to some or all these impacts can be broken into the below categories:

- Sovereign assets – digital and cultural heritage;
- Critical infrastructure;
- Public institutions and intelligence assets; and,
- Research and development assets.

19.1 Sovereign assets – our digital and cultural heritage

Anne Lyons, in a 2018 publication, identified that "we must protect our digital information assets, particularly those that make us a nation legally, culturally, socially and historically."[1] She defined this as 'Australia's National Digital Identity.'

Digitalisation of data is transforming the way cultural institutions such as libraries, archives, museums, galleries and public broadcasters service the public. This digital shift has improved public accessibility to services and the preservation of materials and collections. However, digitising these assets increases their vulnerability, visibility and online exposure. Disruption to Australian societal and cultural values are a consequence of cyber attacks on these assets.

Case study – ransomware and a museum

In May 2019, hackers targeted the Asian Art Museum in San Francisco in a ransomware attack, focusing on data about donors to the Museum.[9] Although unsuccessful in their attempt, cybercriminals, hackers and non-state actors in their pursuit of data will target public and private sectors with the intent to gain high-value information to ransom or to resell. As Anne Lyons outlines from the Australian Strategic Policy Institute, the complexity of the digital and cultural heritage platforms means an alignment between the professional fields of digital preservation and information security is required, and a stronger focus on information governance in order to safely secure sovereign assets is needed.[1]

19.2 Critical infrastructure

There is a diverse portfolio of critical infrastructure sectors which are so vital to Australia that their incapacitation would have detrimental effects on national security, economic and financial impacts, as well as citizen safety. Integral to the functioning of Australia's economy and society, these sectors consist of telecommunications, electricity, gas, water and ports.

Accenture commissioned a threat intelligence report using real-time data from attacks on critical infrastructure operating across the globe and presented the findings in a 2018 report '*Securing Critical Infrastructure*'.[7] The report found that attacks on Industrial Control Systems (ICS) used to manage critical infrastructure have been trending upwards. The 2018 data indicated that 41 per cent of ICS systems globally were targeted by malicious campaigns in the first half of 2018.[7] Looking locally, Australia has seen an increase in attacks on ICS growing from ~24 per cent in 2017 to ~30 per cent in 2018.[7] This indicates that Australia has not yet achieved the capability to prevent or deter ICS attackers.

19.3 Public institutions and intelligence assets

Fundamental to the functioning of the Australian economy and society are the public sector agencies and intelligence departments which engage in serving and protecting our nation. As government platforms begin to transform to a data-driven culture that enables open data for transparency, better service delivery and public participation, the need to secure and ensure appropriate cyber defence frameworks are in place will be essential.

The Australian Signals Directorate (ASD) found that the Australian Government experienced more than 1097 incidents affecting unclassified and classified government networks, in the 2015 to 2018 financial years.[3] Recently, in February 2019, small amounts of non-sensitive data were taken when Australian parliament's network was hacked.

Perceptions of national security are at risk if cyber attacks aimed at the Australian Government continue to occur. Successful breaches to government institutions will have significant consequences including poor service delivery, underperformance of spending, loss of citizen data as well as loss of citizen trust.[4]

19.4 Research and development assets

Education institutions are open and vulnerable to cyber attacks. While the digitisation of the Australian education industry offers new opportunities for schools, universities and students, the need for stronger cyber defences is also required. Cybercriminals are targeting educational institutions to access credentials and personal information as high value data. In the past year, Australian tertiary institutions have been subject to attack with both the Australian Catholic University (ACU) and Australian National University (ANU) victims.[2]

These institutions are a key part of delivering the social infrastructure to the nation, paving the way for future generations and leaders. If educational institutions are continually breached, the credibility, reputation and confidence in those organisations will begin to diminish. With approximately 684,754 international students in Australia as of July 2019,[8] the financial gain and data theft that can be gained from hacking into education institutions is substantial. Protecting both domestic and international students and staff will be the responsibility of the Australian Government and intelligence agencies in order to maintain citizen safety and trust in public institutions.

References for Q19

1 Identity of a Nation, 2018, ASPI. https://www.aspi.org.au/report/identity-nation

2 Universities still need to learn how to get proactive about cybersecurity, 2019, CSO. https://www.cso.com.au/article/664985/universities-still-need-learn-how-get-proactive-about-cybersecurity

3 Good Governance? Why it's time for Australian public sector agencies to examine their network visibility, 2019, CSO. https://www.cso.com.au/article/666695/good-governance-why-it-time-australian-public-sector-agencies-examine-their-network-visibility

4 Recommendation of the Council on Digital Government Strategies, 2014, OECD. http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf

5 Victorian Hospitals Targeted in ransomware cyber attack, 2019, The New Daily. https://thenewdaily.com.au/news/state/vic/2019/10/01/hospitals-cyber-attack

6 Massive ransomware cyber-attack hits nearly 100 countries around the world, 2017, The Guardian. https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

7 Securing Critical Infrastructure, 2018, Accenture. Securing Critical Infrastructure, 2018, Accenture. https://www.accenture.com/t00010101t000000z__w__/au-en/_acnmedia/pdf-96/accenture-securing-critical-infrastructure-new.pdf

8 International Student Data, 2019, Department of Education. https://internationaleducation.gov.au/research/International-Student-Data/Pages/default.aspx

9 Hackers Saw the Asian Art Museum of San Francisco as Ripe for a Ransom Attack. Are other Cultural Institutions Next?, 2019, 2019, Artnet News. https://news.artnet.com/market/hackers-attack-asian-art-museum-san-francisco-1604188

Q21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

21.1 Trust in government capability

If the Australian Government is going to be a trusted custodian of industry data or key collector of industry vulnerability, it needs to demonstrate that it can do it well. When industry shares data about cyber threat they put the economic value and reputation at risk. For industry to build trust in government's ability to be a custodian of commercially sensitive information, Accenture believes the below must be factored in:[1]

- Government must articulate the reason for any collection of industry data and demonstrate the legitimate impacts of not sharing such data;
- Use of data must be explicit and up front, industry must know that any information provided will be used in ways that they know and understand;
- A degree of autonomy must remain with industry to provide the information, empowering industry leaders;
- The integrity of the information/data provided must extend in perpetuity so that industry is satisfied that it cannot be misused;
- Data is secured, the most up to date security provisions are included to prevent cyber threats on the centralised data itself;
- Assurance that the information will not be shared outside of any industry/ government agreement; and,
- Transparency between government and industry through regular and ongoing communications via multiple channels.

21.2 Competitive advantage

Government needs to be acutely aware of the implications of inappropriate use of industry data. Industry may be happy to share data with governments for the greater societal good, but not at the expense of having this exposed to competitors.

In 2018, Ping Identity released results of a global survey looking at customer brand loyalty following a cyber security breach. They found that three-quarters of consumers would stop engaging with a brand online following a breach[3]. This equates to significant revenue loss for the brand concerned and reputational damage that can take years to repair. The reality is that many breaches are not making the news because they are not being reported. And with significant revenue at stake, it is not hard to understand organisations' reticence to share information about cyber breaches, particularly if that information is at risk of leakage to the media more broadly.

21.3 Intellectual property

Companies operating within Australia are subject to intellectual property (IP) laws that provide organisations with safeguards around their IP. The Australian Government will need to consider the interplay between any industry/government information sharing and the inevitable conflict with organisational IP. For industry engaging with the government on cyber security issues the opportunity loss due to potential IP exposure could be just as impactful to industry as a cyber attack itself and counteract the value of industry/government information sharing as a means of cyber security.

21.4 Data without discretion

When the data is collected from private organisations and used for a national purpose, questions need to be solved concerning potential licensing of data used for intelligence, what data to collect, how to collect it and how to store it. There is no doubt that the collation of industry data on cyber threats and vulnerabilities will create a valuable source of 'Big Data' and generate opportunities for modelling, detection and even predictive analytics. However, data collection is only the first action. It is the meaningful interpretation of the data that is key.

Accenture proposes that a 'Cyber Council' formed between industry and government experts in data management co-create an approach. This will not only drive industry engagement but maximise the quality of data collected and therefore the usefulness of interpretations.

21.5 Securing the data

A centralised data pool of all industry vulnerabilities would be a very sought-after commodity for threat actors. Currently, these vulnerabilities are distributed across organisations, limiting the impact to one organisation if the data is attacked. The impact to entire industries if centrally-gathered vulnerabilities are attacked could be catastrophic.

The Australian Government needs to engage with industry and determine the value of collecting this data against the increased risk of centralising it. Industry will need assurance from government that the right security precautions are in place to protect this data from cyber attack. The Australian Government will need to ensure data protection fundamentals are in place by hardening data assets and actively practising data-centric security.[4]

References for Q21

1 Moments that Build Trust, 2018, Accenture. https://www.accenture.com/_acnmedia/pdf-89/accenture-moments-build-trust-digital-business.pdf

2 Government at a Glance 2013, 2013, OECD. https://doi.org/10.1787/gov_glance-2013-en

3 Global Survey from Ping Identity Shows Consumers are Abandoning Brands after Data Beaches, 2018, Ping Identity. https://www.pingidentity.com/en/company/press-releases-folder/2018/global-survey-ping-identity-shows-consumers-abandoning-brands-after-data-breaches.html

4 Achieving Data-Centric Security, 2017, Accenture. https://www.accenture.com/_acnmedia/pdf-65/accenture-achieving-data-centric-security-usweb.pdf

Q26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

As the Australian Government prepares the Australian 2020 Cyber Security Strategy, Accenture believes the critical role of the Australian Public Service (APS) in Australia's cyber security landscape must be addressed.

26.1 Make all APS a key part of the security mix

2019 Accenture research found that public service employees have a long way to go in recognising the role they play in keeping citizens cyber safe[1]. While more than 85 per cent of public sector employees appreciate the importance of cyber security, nearly 90 per cent believe technical cyber security measures are enough to protect citizens' private data. This demonstrates a misconception between the effectiveness of technical security measures and the extent to which individuals must take personal responsibility for their own role in cyber security. To maximise Australia's cyber security all Australian Public Service (APS) staff have to recognise their responsibility in cyber safety.

Accenture's recommendations for governments to increase the cyber security capability and awareness of public service staff are:

- Government leadership need to champion pragmatic anti-risk behaviour to public service staff;
- Develop a tailored security curriculum that follows modern thinking in learning design, such as highly customised to public service roles, delivered in 'bite-sized' modules;
- Add cyber security drills to departments' health and safety programs;
- Create tailored simulations to provide public service staff first-hand experience of an attack such as a moral phishing simulation;
- Socially identify and reward public service staff doing the right thing; and,
- Include all levels of the public service workforce in the ecosystem of cyber security through exchange programs with industry or involvement in the 'Cyber Council' outlined in Question 3 and more.

Developing and maintaining APS capability should be front of mind for the Australian Government when considering its cyber security agenda. Whether by choice or accident, APS staff are custodians of Australian cyber safety and must be both enabled and prepared to fulfil this role.

26.2 Act now for future prosperity

The Australian 2020 Cyber Security Strategy is an opportunity to maximise the prosperity and future growth of Australian society. While cyber security is a global issue, it necessitates a co-ordinated local response that is responsive to the rapidly evolving state of cyber threats. It is imperative that the Australian Government does not consider itself alone in responding to these threats and attention is given to an active framework co-created with industry and citizens. A comprehensive Cyber Council model provides the Australian Government the support it needs across the cyber ecosystem to push an Australian cyber agenda that is modern, and hardens Australia's cyber security for future society, critical systems and national interest.

References for Q26

[1] People are at the heart of protecting citizen data, 2019, Accenture. https://www.accenture.com/au-en/insights/public-service/the-peoples-defence

Appendix A
The Cyber Threat Landscape

26.1 The evolving cyber threat environment

In Accenture's 2019 '*The Cost of Cybercrime*' study, we combined research from across 11 countries in 16 industries.[1] We interviewed 2,647 senior leaders from 355 companies and drew on the experience and expertise of Accenture Security to examine the economic impact of cyber attacks.[1] We found that cyber attacks are changing due to:

- **Evolving targets:** information theft is the most expensive and fastest-rising consequence of cybercrime—but data is not the only target. Core systems, such as industrial control systems, are being attacked in a powerful move to disrupt and destroy.
- **Evolving impact:** while data remains a target, theft is not always the outcome. A new wave of cyber attacks sees data no longer simply being copied but destroyed —or changed—which breeds distrust. Attacking data integrity is the next frontier.
- **Evolving techniques:** cybercriminals are adapting their attack methods. They are using the human layer—the weakest link — as a path to attacks, through increased phishing and malicious insiders.[3] Other techniques, such as those employed by nation-state attacks to target commercial businesses, are changing the nature of recovery, with insurance companies trying to classify cyber attacks as an "act of war".

26.2 Threat actor categories and their motivations

26.2.1 Cyberespionage

Cyberespionage is the compromise of online systems to gain a strategic advantage and can encompass a broad set of objectives, including but not limited to:

- Acquiring intellectual property to gain competitive advantage for a nation state;
- Degrading other nations' capabilities; and,
- Influencing or understanding a target's political and strategic decision-making to support the attacking country's own policy.

The specific intents, motivations and objectives of a cyberespionage threat group will vary according to the nation it is associated with and that nation's foreign policy goals. The difficulties in attributing attacks embolden nations to conduct cyberespionage and influence activities against traditional enemies and allies alike.

Australia's alliances and its geo-strategic circumstances make for a complex threat environment, but also provide unique opportunities to leverage the resources of powerful allies and contribute the dividends of a history of cyberespionage excellence and an advantageous geographical position.

26.2.2 Cybercrime

Cybercrime is the compromise of online systems for financial gain. Cybercrime can encompass a broad set of objectives, including but not limited to:

- Stealing intellectual property for financial purposes;
- Stealing personally identifiable information (PII) or protected health information (PHI) to sell on DarkNet markets;
- Installing ransomware for financial gain;
- Accessing credit card information for financial gain; and,
- Accessing data to subsequently use to extort an organisation.

Generally, cybercriminals target weak security systems and/or individuals to harvest personal information. An example of this was seen during the WannaCry attack which locked thousands of machines globally. As a digitally advanced nation with a large number of public and government services available online and an ageing population Australia is a prime target for increasingly sophisticated cybercriminals.

26.2.3 Cyberactivism

Cyberactivism or hacktivism is a form of protest carried out by cyber means. The aim is to compromise online systems to further or support ideological or political motives. It includes leaking confidential business or government documents or performing distributed denial of Service (DDoS) attacks on business or government networks to support hacktivist causes, which are usually political or social in nature.

26.2.4 Insider threat

Snowden and Wikileaks are examples of attacks that caused significant impact to national interests in recent years. All were perpetrated or enabled by insider threats and all undermined confidence in government. Insider threat of this nature is often a type of cyberactivism and actors are usually ideologically or morally driven.

Contrarily, insider threat can also be driven from personal vendetta's, as discussed in Question 4 in the case study 'Maroochy Shire QLD Sewerage spill.' In this Australian based incident an individual made an attack after being turned down for a new job. Insider threats are complex as the motivations can be multifactorial and the potential impact sizeable.

26.2.5 Advanced Persistent Manipulators

This threat actor group coined by analyst Clint Watts of the Foreign Policy Research Institute and George Washington University, describes threat entities[2] that have abundant resources to conduct "an extended, sophisticated, multi-platform, multi-media information attack on a specified target," sometimes combining online influence campaigns with real-world activities such as rallies.[3] The motivations for this type of threat actor varies greatly by who/what is funding the activity.

26.3 Types of threats

While the ways cyber threat actors operate are maturing and becoming more 'professionalised' in their approach, much of the current damage inflicted by cyber attacks still occurs through unsophisticated actions. The below outlines the key threat types Accenture believes need to be considered for the 2020 Cyber Security Strategy.

26.3.1 Hacking hearts and minds - the disinformation threat

Social media remains a battleground for the hearts and minds of worldwide audiences, as it can be used for disinformation and other forms of information operations to try to sway opinion and influence policy.[3] While there are many channels threat actors can distribute information operation attacks, social media is easily accessible and ubiquitous to a digital society making it a key channel to be aware of.

In addition to deliberate disinformation, information operations also include propaganda (the spread of information to promote a political cause) and misinformation (the spread of inaccurate information without an intent to deceive). Disinformation and other information operations cyber threats can act via "white" methods (broadcasting one's message openly through state media), "grey" methods (placing information in other sympathetic media), and "black" methods (using hackers, trolls and honeypots).

While disinformation has not traditionally been considered a cyber threat, without a co-ordinated and global response to information operations this type of activity could become a significant threat to Australia's society and way of life.

Advanced Persistent Manipulators regularly employ "trolling-as-a-service" to aggregate audience data and disseminate targeted and often inauthentic messaging, sometimes involving altered data.[3] Attempts to fight this large scale and persistent disinformation in court are long and expensive, and as Quinta Jurecic from Lawfare discussed in her article '*Where is the world is Elena Khusyaynova?*' the perpetrators may never be brought to justice.[4]

26.3.2 Information operations and distributed denial of service (DDoS)

Cyber-enabled information operations (CyIO) that can exploit the openness and speed of communications in cyberspace. DDoS as described by Cloudfare, a global cloud based cyber security service, is an unsophisticated and easily achievable way of perpetrating a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.[5]

Advances in technology, such as artificial intelligence and 5G communications, will provide new opportunities for threat actors to take advantage of and influence global political events.[3]

26.3.3 Adversarial Artificial Intelligence

In the report '*Know Your Threat: AI Is the New Attack Surface*',[7] Accenture Labs discusses the adversary opportunity opened up by increasingly complex machine-learning models, especially image content and classification, natural language processing (NLP) and industrial control systems (ICS).

As threat actors focus more on interference with AI modelling, they are likely to deploy adversarial AI, corrupting the ability of machine learning algorithms to interpret system inputs and exercising control over their behaviour. To do this, attackers may create adversarial examples to break the model's performance, using deep learning models known as Generative Adversarial Networks (GAN). Adversarial AI using deep-learning applications in natural language processing could enable the manipulation of algorithms that determine sentiment, gather intelligence, or filter for spam and phishing.[6]

26.3.4 Phishing/spear phishing

Phishing remains an ever-present cyber risk. Threat actors who use phishing are developing their capability in social-engineering, increasingly tailoring attacks to trick a user of the system into opening a malicious file or to send sensitive data to a malicious third party. Though phishing has been prevalent since the dawn of the internet, it is still the most commonly used cyber attack approach to date by all threat groups. Phishing campaigns are a method of delivering malicious files and have been seen in many famous attacks such as the malware attack from BlackEnergy 2 which was delivered through phishing and was designed to perform reconnaissance on the network.

26.3.5 Malware

Malware is malicious software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system. Malware is particularly effective when targeting Infrastructure Control Systems (ICS) and poses the largest economic threat to critical infrastructure across the world.[7] Blackenergy 2, and Havex are some well known examples of custom-crafted malware that were specifically designed to disrupt or monitor ICS systems. These were quickly followed in 2017 by two new ICS-specific malware samples: Trisis and Crashoverride. These two pieces of malware were designed to specifically target and disrupt electric grid operations and to target and disrupt Safety Instrumented Systems (SIS) resulting in a potential loss of human life. Below are the main categories of malware to be aware of:[1, 3, 7]

- **Cryptominers** – are a form of malware that will use a company's resources to mine crypto currencies. Statistics show that the percentage of ICS computers attacked by malicious programs designed for mining cryptocurrencies has grown sharply in the first half of 2018 reaching 6 per cent – 4.2 per cent more than the previous six months. Cryptomining provides a high risk to ICS as it can slow down the system which can lead to potential issues for monitoring and safety controls.
- **Ransomware** – a form of malware that is designed to lock a company's system until a ransom is payed to obtain the unlocking private key. The percentage of ICS computers on which ransomware attacks were blocked grew from 1.2 per cent in 2018 to 1.6 per cent in 2019.
- **Worms** – are a malware computer program that replicates itself in order to spread to other computers. Worms are usually used to monitor or disrupt an industrial system. The most well known example of a worm is the Stuxnet virus which interfered with the ICS controls of an Iranian power plant.

26.3.6 Botnet

Albanese et al in their paper '*Adaptive Cyber defences for botnet detection and mitigation*' describe botnet as a group of remotely controlled workstations that can be used by a malicious actor to perform large-scale attacks on a company's resources.[8] The adoption of the Internet of Things (IoT) has driven several industries, such as smart manufacturing, to adopt and embrace the advantages of connecting to the Internet. Botnets can be utilised by attackers to perform distributed denial of service attacks on other companies.[16]

References for Appendix A

1 2019 Ninth annual cost of cybercrime study, 2019, Accenture. Ninth annual cost of cybercrime study, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

2 Advanced Persistent Manipulators, 2019, Collin Watts. https://securingdemocracy.gmfus.org/wp-content/uploads/2019/02/APM-Clint-1.pdf

3 iDefense Cyber Threatscape report, 2019, Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

4 "Where in the World Is Elena Khusyaynova?", October 26,2018, Quinta Jurecic. https://www.lawfareblog.com/where-world-elena-khusyaynova.

5 What is a DDoS Attack?, 2019, Cloudflare. https://www.cloudflare.com/en-au/learning/ddos/what-is-a-ddos-attack

6 Know your threat: AI is the new surface attack , 2019 Accenture. https://www.accenture.com/_acnmedia/accenture/redesign-assets/dotcom/documents/global/1/accenture-trustworthy-ai-pov-updated.pdf

7 Securing Critical Infrastructure, 2018, Accenture. Securing Critical Infrastructure, 2018, Accenture. https://www.accenture.com/t00010101t000000z__w__/au-en/_acnmedia/pdf-96/accenture-securing-critical-infrastructure-new.pdf

8 Adaptive Cyber Defenses for Botnet Detection and Mitigation, 2019, Massimiliano Albanese, Sushil Jajodia, Sridhar Venkatesan, George Cybenko, Thanh Nguyen. https://link.springer.com/chapter/10.1007/978-3-030-30719-6_8

Authors and acknowledgments

About Accenture Security

Accenture Security helps organisations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organisation's valuable assets, end-to-end. With services that include strategy and risk management, cyber defence, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us **@AccentureSecure** on Twitter.

About Accenture's Cyber Fusion Centre

Accenture has recently opened a Cyber Fusion Centre in Sydney, Australia. As part of our global network of Cyber Fusion Centres, this is a world leading cybersecurity facility to help both Government and Commercial organisations innovate new intelligence-driven solutions so they can effectively defend against the ever-evolving threat landscape. The centre will combine our managed detection and response capability with our advanced threat hunting, red team, intelligence and incident response functions. The Cyber Fusion Centre is a focal point for continuous, collaborative innovation and sharing—melding the power of our client's teams, Accenture's security expertise as well as university and ecosystem alliance partners including Microsoft, Splunk and Palo Alto networks. Contact **Michael.shepherd@accenture.com**

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 492,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**.

Contributing Authors

Michael Dowling
Security Lead for Resource Industry Group

Johanna Elms
Management Consulting Manager for Government

Raymond Griffiths
ANZ Operational Technology Security Lead

Anthony McDougall
Technology and Architecture Leadership for Government

Zoe Thompson
Security Consulting Manager for Government

Contact Authors

Ann Burns
Resources (Critical Infrastructure) Lead
[redacted]

Joseph Failla
Accenture ANZ Security Lead
[redacted]

Chris McNally
Cyber Security Lead
[redacted]

Melissa Waldron
Home Affairs Account and Consulting Lead
[redacted]

191541