Australia's 2020 Cyber Security Strategy

Australian Government

A call for views

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600

Submissions are welcome at

https://homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020/submission-form

Australia's 2020
Cyber Security Strategy

A call for views

Australian Government

Table of Contents

Foreword

Cyber security has never been more important to Australia's economic prosperity and national security. In 2016, the Australian Government delivered its landmark Cyber Security Strategy, which invested $230 million to foster a safer internet for all Australians. Despite making strong progress against the goals set in 2016, the threat environment has changed significantly and we need to adapt our approach to improve the security of business and the community.

Cyber criminals are more abundant and better resourced, state actors have become more sophisticated and emboldened, and more of our economy is connecting online. Cyber security incidents have been estimated to cost Australian businesses up to $29 billion per year and cybercrime affected almost one in three Australian adults in 2018. At the same time, serious cyber incidents like WannaCry, Cloud Hopper and the intrusion into Australia's parliamentary networks illustrate the threat to our economy, democracy and way of life.

For businesses, a more secure cyberspace will support the delivery of digital services that Australians have come to rely on. Cyber security will underpin our future economic growth and ensure we remain competitive globally as Australian enterprises innovate and find new ways of creating value for their customers.

For nationally significant systems, such as those that control our power and water, Australia must position itself as a world leader in cyber threat detection, prevention and response. This means government and industry will need to work closer together than ever before.

For individuals and families, I want to ensure more support and assistance is provided to keep them safe online. Every Australian should have the confidence that they can keep themselves and their family safe while taking advantage of the online world.

I encourage all Australians to have a say in this discussion paper – from small businesses to large corporations, tech experts to interested individuals. Together we can build on what we have already achieved and take the next steps towards a stronger and more prosperous Australia.

I look forward to hearing your contributions and insights.

The Hon Peter Dutton MP
Minister for Home Affairs

5 September 2019

Introduction

The internet is an essential part of life for many Australians. We use it to work, stay in touch, access entertainment, pay the bills and manage our finances. At the same time, more of the things around us are connecting online, including our cars, household appliances and industrial machinery. The benefit this brings is enormous, but it also exposes us to new threats from those who wish to do us harm.

Australia's 2016 Cyber Security Strategy set out Government's plan to strengthen our cyber resilience and security. The Strategy, backed by a $230 million investment, built Australia's cyber security foundations and raised national awareness of online threats. Since 2016, we have opened the Australian Cyber Security Centre within the Australian Signals Directorate to be the single point of cyber expertise for the Australian Government. We have also formed Joint Cyber Security Centres across the country to work more closely with industry, and we have created a 24/7 Global Watch to respond to critical cyber incidents.

The rapid pace of change in cyberspace and the extent of our reliance on the internet means we cannot be complacent. A loss of an essential service like electricity, water or transport has the potential to cripple the economy, cause social unrest and, ultimately, damage our welfare and way of life. There are also many who seek to undermine our strong and enduring institutions. Recent incidents such as compromises of the Australian parliamentary networks, universities and key corporate entities illustrate that the threat continues to be significant. Even smaller scale cyber incidents affecting families and local businesses often lead to financial loss, business interruption, identity theft and psychological stress.

We want to explore with you how Australia can position itself to meet cyber threats, now and into the future. In forming a view, we will need to consider whether responsibilities are appropriately assigned in keeping everyone safe. This will require a thoughtful discussion about how Government, businesses and individuals can share responsibility for cyber security in the future to get the best outcome for everyone.

For the Strategy to be successful, we need to develop and deliver it in partnership with the Australian community. This discussion paper seeks views from all Australians about how to grow Australia's cyber security and future prosperity. Cyber security affects us all and we are seeking views from small, medium and large businesses, industry bodies, academia, advocacy groups, not for profits, government agencies, community groups and members of the public. We have posed a series of questions you may wish to answer as you offer your thoughts.

By working together, governments, academia, industry and the community can strengthen our nation's cyber resilience across the economy to ensure we prosper as a nation and protect our interests online.

Where we are now

We have made a lot of progress since the release of the 2016 Cyber Security Strategy. We have:

- Opened the Australian Cyber Security Centre to bring together the Government's cyber expertise in one location and strengthen our ability to meet current and emerging threats.
- Built stronger partnerships with businesses, governments and academia, including through the establishment of Joint Cyber Security Centres in five capital cities.
- Established a 24/7 Global Watch to respond rapidly to cyber incidents and launched cyber.gov.au as a new 'one-stop-shop' for cyber security advice.
- Shown international leadership by appointing an Ambassador for Cyber Affairs, strengthened our commitment to act in accordance with existing international law and agreed norms of behaviour in cyberspace, and supported activities that build cyber capacity across ASEAN and the Pacific.
- Publicly attributed significant cyber incidents to multiple nation states.
- Supported our domestic industry through AustCyber (the Australian Cyber Security Growth Network), Austrade's Landing Pad Program and a $50 million investment in the Cyber Security Cooperative Research Centre.
- Invested in skills and education, including through Academic Centres of Cyber Security Excellence at the University of Melbourne and Edith Cowan University, and national Certificate IV and Advanced Diploma qualifications.

Further detail on progress against the 2016 Strategy is at Appendix A.

While we have delivered these outcomes, we have also noticed growth in the scale and severity of malicious cyber activity. Cyber criminals continue to target Australians and are enabled by tools that are cheap and widely available. The most basic do not require a high level of technical knowledge, making it easier to undertake criminal activities. Valuable personal information, which can be used for financial fraud or other serious crimes, is a major target.

State actors are also growing more organised, confident, and sophisticated in using cyber espionage and interference to promote their national interests. Malicious cyber activity includes efforts to influence public opinion and interfere in democratic processes. This includes the 'hack and release' of sensitive information, which is intended to embarrass the target and damage their reputation with the public.

While new threats are constantly appearing, known vulnerabilities and basic techniques that have been used for decades also remain effective against networks that lack baseline

cyber security. Adversaries of all kinds routinely scan the environment for easy targets. Many Australians continue to fall victim because they fail to observe, or are unaware of, basic online security practices.

Against this backdrop, Australia's critical systems, including in the energy, telecommunications and transport sectors, are becoming increasingly digitised. International cyber incidents have disrupted power grids, degraded public health and transport systems, and damaged physical infrastructure. These new threats, if realised in Australia, could threaten physical safety, economic security, and the continuity of Government and its services.

Australians are relying on the internet and digital services more than ever. Technologies such as automation, artificial intelligence, virtual reality and the internet of things will continue to transform the way we live, work and interact with each other. These changes bring unprecedented opportunities for all Australians. However, these changes also make us more reliant on technology and potentially more vulnerable to malicious cyber activity.

We welcome your views on

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

Cyber Security by the Numbers

- **$2.3 billion** was stolen by cyber criminals from Australian consumers in **2017**.[1]
- **964 data breach notifications** were made under the Notifiable Data Breaches scheme from April 2018 to March 2019, **60 per cent** of which were **malicious or criminal attacks**.[2]
- **53,474 reports** were received by the Australian Cybercrime Online Reporting Network in the **2017/18** financial year, and **64,528** in the **2018/19** financial year.
- **2500 per cent increase in the sale of ransomware** on dark net sites between 2016 and 2017, with basic tools costing as little as $1.[3]
- **250 per cent increase** in the share of inbound emails that were **phishing messages** in 2018 alone.[4]
- **$2.1 billion** per year, at least, is the estimated economic **impact of identity crime in Australia**.[5] 80 per cent of victims receiving assistance from IDCare, Australia and New Zealand's national identity and cyber support service, reported a psychological impact.

1 Norton 2017, *Norton Cyber Security Insights Report*, available from https://au.norton.com/cyber-security-insights-2017.
2 Office of the Australian Information Commissioner, *Notifiable Data Breaches Scheme 12-month Insights Report*, available from https://oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf.
3 Carbon Black 2017, *The Ransomware Economy*, available from https://www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf.
4 Microsoft 2018, *Security Intelligence Report, Volume 24*, available from https://www.microsoft.com/en-us/security/operations/security-intelligence-report.
5 Australian Institute of Criminology 2017, *Estimating the costs of serious and organised crime in Australia 2016-17*.

Positioning ourselves for the future

Changes in the cyber security environment mean we should consider whether we can better position ourselves to deter, detect and respond to threats as they emerge. Answering this question means first determining the most appropriate role for governments, industry and the community in keeping Australia cyber-secure. Cyber security has always been a shared responsibility, but it is worth asking whether the balance of responsibilities among these groups is right.

End-users, such as individuals and small businesses, carry a high level of risk in managing their online activity and often bear the loss caused by malicious activity. They are often not best placed to identify or respond to cyber risks, or assess the gravity of the consequences should a cyber risk be realised. This applies to most individuals and small businesses, but can also be true of large scale enterprises.

In contrast, providers of goods and services that help customers access or benefit from the internet tend to have a better understanding of cyber risks and their potential consequences. Some hardware manufacturers, software vendors, owners of infrastructure and internet based platforms have sophisticated protections in place, while others are far less mature in supporting the cyber security of their customers.

Finally, the role of Federal, state and territory governments in cyber security has traditionally been limited to protecting government networks, enforcing the law and offering advice. The owner of a compromised network can invite Government to assist in remediation when a nationally significant cyber incident occurs, but is under no obligation to do so. Businesses are generally only required to report significant compromises of personal information, so Government may be unaware of significant incidents that threaten Australia's national security or economic prosperity unless the company reports the incident or it is noticeable to the public.[6]

The implication of current arrangements is that end-users carry a significant portion of the risk, and Government has a limited role in protecting a large number of systems critical to our way of life. Whether these outcomes are correct is one of the most fundamental questions we need to explore. Our current settings support personal choice and responsibility, and encourage business investment in the digital economy. An alternative approach might be to prioritise cyber security by transferring responsibility for managing a greater portion of cyber risks away from end-users and onto industry and business.

6 Listed companies may also be obliged to publicly disclose any incident (including security breaches) that impacts on their stock price. Financial entities covered by the Australian Prudential Regulation Authority's information security rules have an obligation to notify the regulator of material breaches.

We welcome your views on

2 Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

3 Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

Government's role in a changing world

Another important question is whether Government's role should change to offer greater assistance to Australian businesses to defend against highly sophisticated malicious actors (see case study, overleaf). State actors target Australian businesses for a range of reasons, including access to intellectual property and espionage. In these situations, it might not be possible for businesses to fully defend themselves given the skills and expertise of those targeting them. The Government is most concerned about threats to Australian businesses that provide essential services, such as energy, water, telecommunications and transport.

The Government currently uses its cyber security capabilities within a legislative framework that was established before the internet became a foundational element of our economy, and without a modern perspective on how malicious cyber activity crosses traditional geographical borders.[7] Government's activity is also regulated strictly by law and subject to extensive external and independent scrutiny to protect the privacy of Australians.

Maintaining the confidence of the Australian community is the first priority when considering how and when Government should use its cyber security capabilities. With this in mind, we are seeking your views on whether Government's role could evolve to better meet your expectations of security while maintaining your trust. Key to this is whether you think Government could do more to confront cybercrime and protect the networks that underpin our way of life, or whether you think the current arrangements are right. If you think there is scope for Government to do more, we are seeking your views on how it could do this in a way that means you remain confident your rights as an Australian citizen are protected.

We welcome your views on

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

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

7 This issue is also being considered by the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Richardson Review). Further information is available from https://www.ag.gov.au/NationalSecurity/Pages/Comprehensive-review-of-the-legal-framework-governing-the-national-intelligence-community.aspx.

Case Study: How can Government proactively address national cyber threats?

The Australian Government currently provides cyber security advice to the community, businesses and governments, prosecutes cyber criminals and disrupts cyber criminals operating outside Australia. Government also has an incident response capability which can be used in serious cases. Under existing legislative frameworks, Government can only take direct action to prevent or respond to cyber security incidents with the permission of network owners (including other government agencies). This takes time and gives malicious actors an advantage. In national emergency situations, it may be appropriate for Government agencies to take swifter action.

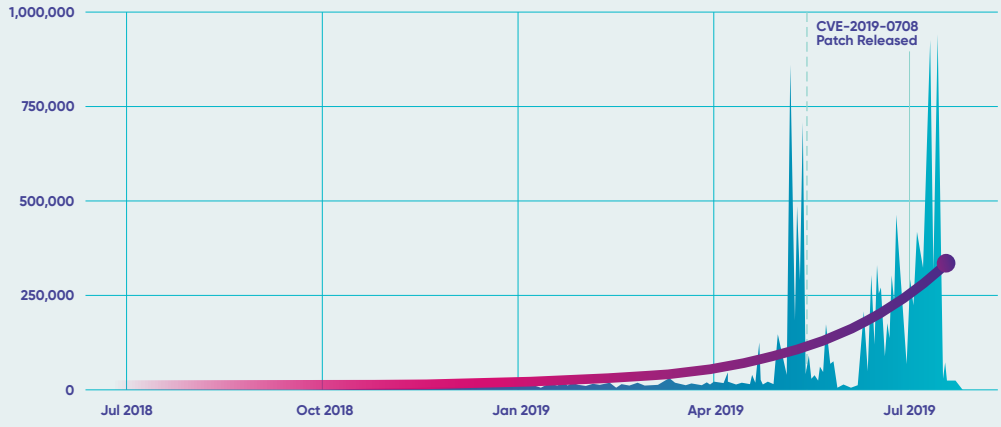
A good example is the 2019 BlueKeep vulnerability affecting older versions of Windows operating systems. BlueKeep is a very serious vulnerability because it is 'wormable', meaning it can spread between networks without anyone downloading a file or clicking on a bad link.

The Australian Cyber Security Centre estimates that there could be up to 50,000 vulnerable machines in Australia right now. Given the seriousness of the situation, it may be appropriate for Government to proactively identify any vulnerable systems to assess Australia's exposure and better assist the community. However, this is not an option open to Government under the current laws, and the risks to our critical systems remain unknown. At the same time, we know that malicious actors are undertaking proactive scanning for the BlueKeep vulnerability, which is a strong indication of intent for future attacks (see illustration below).

At the moment, Government is relying on vulnerable organisations to respond to public warnings from the Australian Cyber Security Centre. Past experience, such as the WannaCry incident, shows us that not everyone responds to these warnings and that this could have serious consequences at a national scale.

Number of public scans to detect the BlueKeep Vulnerability

Blue shaded area shows total daily activity; purple line shows the overall activity trend.



Source: Rapid7 Labs & GreyNoise Intelligence

Enterprise, innovation and cyber security

The technology sector is the cornerstone of our growing digital society and digital economy. It designs, manufactures and manages our online experiences. Businesses drive Australia's digital economy, which is essential to our prosperity. If something involves the internet, it will involve an innovative business, either from Australia's world class domestic cyber industry or from overseas.

Government plays a role in facilitating private sector success, be they individuals, small to medium or large businesses. Clear and reasonable rules that protect consumers and keep risky businesses out of the market are good for everybody. But there is always a balance Government must strike – obligations that are unclear or onerous can discourage innovation and reduce our international competitiveness. On the other hand, the rules that protect and support Australians should keep pace with the extreme rate of technological change in rapidly evolving sectors of the economy.

The variability in the security of cyber goods and services raises the question of whether it is reasonable to expect providers to do more to protect their customers. Adding to this is the question of whether a purchaser is adequately equipped to protect themselves. It may indicate that strengthened protections are not feasible in some cases because they would impair the operation of a product or make it cost prohibitive. This suggests a choice between potentially preventing consumers from accessing products that expose them to a high degree of risk, and allowing a consumer to accept this risk if they believe it is outweighed by the benefit the product brings. This then makes a consumer's ability to make an informed choice important in framing a way forward.

To identify any gaps, we are interested in exploring with all stakeholders what existing legislation is available to ensure consumers can be confident products and services include reasonable cyber security protections. Importantly, we also want to examine whether such legislation is proactive in providing and enforcing such protections for consumers, which can be either individuals, businesses or governments.

In most cases, the liability of suppliers is limited by complex contractual clauses, leaving the customer bearing the cyber security risk. In some cases there are statutory protections – such as consumer and privacy laws – but it is unclear whether these laws provide adequate incentive for companies to invest in necessary cyber protections. There are also many examples where these laws may not apply, such as business-to-business transactions, which can make it very difficult for enterprises to have confidence in the cyber security of their supply chain.

Another potential gap is cyber security requirements for providers of essential services. In some cases there are already mature cyber security requirements (see, for example, the *Telecommunications Sector Security Reforms*). In other cases, however, there are minimal or highly variable requirements with different standards of enforcement. This is especially true when services are provided across different levels of government or by many smaller organisations (like water and sewerage services). A better approach may be consistent but flexible cyber security laws for critical systems (see case study below).

Case Study: Europe's Network and Information Security Directive[8]

The Network and Information Security (NIS) Directive is the first piece of EU-wide cyber security legislation. The NIS Directive was adopted in 2016 and because it is an EU directive, every EU Member State has started to adopt national legislation, which follows or 'transposes' the Directive. The NIS Directive gives EU countries some level of flexibility to take into account national circumstances, for example, to re-use existing organisational structures or to align with existing national legislation.

The NIS Directive has three parts:

1. **National capabilities:** EU Member States must have certain cyber security capabilities such as a Cyber Security Incident Response Team (CSIRT).
2. **Cross-border collaboration:** EU Member States must participate in coordination forums such as the operational EU CSIRT Network and the Strategic NIS Cooperation Group.
3. **National supervision of critical sectors:** EU Member States have to supervise the cyber security of those who provide essential services in their country. There is 'before the fact' or proactive supervision in critical sectors (energy, transport, water, health and finance sector) and 'after the fact' or reactive supervision for critical digital service providers (internet exchange points, domain name systems).

As the risks and consequences from malicious cyber activity rise, we are seeking your feedback about whether Government's approach to cyber security laws needs to change. Both stronger enforcement of existing laws and new requirements could be considered. If change is needed, Government would favour the option that delivers the largest long-term benefits for society while minimising any upfront costs for industry.

8 Adapted from https://www.enisa.europa.eu/topics/nis-directive

We welcome your views on

6 What customer protections should apply to the security of cyber goods and services?

7 What role can Government and industry play in supporting the cyber security of consumers?

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

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

10 Is the regulatory environment for cyber security appropriate? Why or why not?

11 What specific market incentives or regulatory changes should Government consider?

A trusted marketplace with skilled professionals

Increased reliance on technology underscores the need for higher standards of cyber security to maintain the availability and integrity of critical services. This trend means demand for secure products and services as well as skilled cyber professionals will continue to increase. However, it is difficult for many businesses and consumers to understand what level of security is embedded in digital products or what level of service a professional can provide. Cyber security decisions made by businesses and consumers, when added up together, can have implications for Australia's economy and national security.

A trusted market of secure technologies, products, services and professionals is critical for improving cyber security outcomes in Australia. By 'trusted market' we mean an open, transparent, diverse and competitive technology market, where vendors include cyber security protections as standard and buyers clearly understand any risks. Ideally, digital products and services should have security built in 'by-design', so that users do not need to have any expert knowledge. Similarly, businesses of all sizes need to be able to trust their suppliers and get access to expert advice when needed. Globally it appears that the mechanisms and incentives for this to occur, such as visible and trusted industry standards, do not yet exist in most cases.

Access to skilled professionals is an important part of a 'trusted market'. Government continues to receive feedback about a cyber security skills gap in Australia. AustCyber estimates that there were 2,300 fewer skilled cyber security professionals than required in Australia in 2018. Up to an additional 17,600 will be needed by 2026. Some stakeholders also have raised concerns about whether the education and training system is meeting the needs of the cyber security sector, and whether sufficient data is available on this issue. Part of the problem could be confusion about what qualifications are needed for what cyber security jobs.

Another component of a trusted market is cyber security insurance. Insurance can help policy holders prevent, respond and recover from cyber incidents. Anecdotal evidence suggests there is a relatively low take-up of a limited range of cyber related insurance products amongst Australian businesses. There are other indications that the cyber insurance market is relatively immature in Australia, such as the lack of standard terms of coverage in cyber insurance contracts. Difficulties in quantifying the risks and potential losses from future cyber incidents could be a barrier to growth in this area.

We welcome your views on

12 What needs to be done so that cyber security is 'built in' to digital goods and services?

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

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

15 Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

A hostile environment for malicious cyber actors

Given the scale and reach of the threats across the economy, we currently place a heavy emphasis on tending to victims through incident response. This can come at the expense of stopping threats from getting to the victim in the first place. We won't be able to arrest our way out of this situation, so increased law enforcement capability and capacity will help, but not solve the problem.

The current approach relies on a victim's own decision-making skills to prevent the kind of damage that happened from campaigns such as WannaCry. This type of ransomware is just one example of a threat that could be countered on a much larger scale if preventative measures are put in place. Such measures would aim to make Australian networks harder to exploit, although we can never be totally cyber secure.

On one side there are low risk, passive measures that are already standard practice for most sizeable organisations. At the other end are offensive measures to disrupt, deny or degrade the computers or computer networks of our adversaries. These tightly regulated tools belong exclusively to the Australian Government and are high cost and high risk.

Between those two ends of the spectrum lie a range of actions – mid-level capabilities. Such measures can include gathering information on actors targeting Australia, sharing advice on hostile activity between entities involved in defending networks or blocking known malicious actors. Australia already works closely with international partners to share information and build support for international rules and norms to govern the responsible use of cyber space.

International models – active defence in the United Kingdom

The UK Government is a leading international example of how such active measures can be used to protect citizens. The UK is making their nation a much harder target for state sponsored actors and cyber criminals by increasing the resilience of their networks. They want to defeat the vast majority of high-volume, low-sophistication malicious activity on UK networks by blocking malware communications between hackers and their victims. They are also looking to increase the scale of their capabilities to disrupt serious state sponsored and cybercriminal threats. This is a strategy focussed on prevention, not cure.

Further information is available at https://www.ncsc.gov.uk/section/products-services/active-cyber-defence.

The Government will always play its part in countering the most sophisticated and dangerous threats to the nation, but it is becoming increasingly important for this to be supported through partnerships and collaboration with industry. The number of critical privately owned or operated systems at high risk of malicious activity is growing and therefore the number of close partnerships between Government and industry may need to grow. In the past, Government's focus has generally been limited to food, water, health, energy, communications, transport, banking and the public sector, but this will need to expand to include more digital infrastructure, such as data centres and online marketplaces.

If Government needs to provide ongoing and sustainable services to owners of critical systems, then the cost may need to be recovered through direct charges or other alternative funding models, rather than relying on general taxation revenue.

Cyber risks to essential services

The industrial control systems used in delivering essential services like water, energy and transport are evolving towards greater connectivity and internet dependence. This can present sophisticated adversaries with new opportunities to exploit these critical systems. Despite the many benefits internet connectivity provides, administrators of industrial control systems need to remain alert to adversaries seeking to interfere.

The December 2015 cyberattack on the Ukrainian power grid was the first known instance of a cyberattack on power infrastructure, which left over 200,000 people without power for up to six hours. The 2017 NotPetya and Wannacry attacks – attributed to Russia and North Korea respectively – had broad impacts including across the financial, transport and healthcare sectors. The 'Triton' attack against a Saudi petrochemical plant in late 2017 saw the targeting of systems that protect human life.

We welcome your views on

16 How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

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

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

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

20 What funding models should Government explore for any additional protections provided to the community?

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

A cyber-aware community

Australians need the right knowledge to make cyber-smart consumer choices. We need to know when to demand better cyber security features from the products and services we use. And we need to know how to be more consistent in practicing secure online behaviours.

Human behaviour is the most significant weakness exploited in cybercrime. Successful attacks often rely on an end-user's lack of cyber security understanding, using methods such as mass phishing email campaigns as well as the more targeted attacks such as spearphishing or whaling. The FBI's Internet Crime Complaint Center's 2018 Crime Report revealed they received just over 20,000 reports of Business Email Compromise attacks with adjusted losses of over US$1.2 billion that year alone.

We aren't born with knowledge of cyber security. It is through education that risks are appreciated and the measures to mitigate them are learned. But like all other forms of security, awareness is a complement to, not replacement for, the availability of secure features. For example, drivers are provided with a seat belt in addition to education about the importance of road safety and incentives to use the seat belt. And the same expectations and requirements we have where safety is paramount should apply in cyberspace.

The question then becomes how to empower consumers to demand services and products that have been designed with cyber security in mind. We will need to leverage community and industry partnerships to gather the evidence about what behaviour change initiatives work best and roll them out at scale. Secure online behaviours should be as common as locking the door at home. But user-awareness across both private and business environments is generally still too low.

We welcome your views on

22 To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

23 How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

24 What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

25 Would you like to see cyber security features prioritised in products and services?

Is Australia Cyber Aware?

- **14 per cent of Australians** say they haven't taken any steps to protect themselves online.[9]
- **1 in 4** millennials share passwords across all online accounts.[10]
- **80 per cent** of Android users and **23 per cent** of iOS users haven't installed the latest updates.[11]
- **21 per cent** of Australians don't know that their smart devices can be hacked.[12]

Other issues

We welcome any feedback on any issues that have been missed in this discussion paper or any other issue that Government should consider.

We welcome your views on

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

9 2018 Norton Lifelock Cyber Safety Insights Report
10 2017 Norton Cyber Security Insights Report Global Results
11 Symantec, Internet Security Threat Report Volume 23 (April 2018)
12 2018 Norton LifeLock Cyber Safety Insights Report

Taking things forward

Advanced digital economies must be protected by robust and appropriately resourced cyber security arrangements. Our hope is for all Australians to play a role in building cyber security into our online society and economy, empowering us to prosper.

A new Cyber Security Strategy will take us a long way forward, but it would be unrealistic to expect it to solve all problems. Australia's 2020 Cyber Security Strategy cannot be a magic bullet for all the complexities arising from the digital age. A defined scope that focuses on the security of digital activity ensures it can deliver meaningful and targeted change to better protect Australians. This acknowledges complementary pieces of work occurring within the Australian Government across the technology spectrum.

We want to test and refine our high level ideas to ensure we have scoped the right problems and the right solutions. We will then develop the detailed actions needed to deliver on these objectives. Once the Strategy is finalised, we will also develop a robust evaluation plan so we can measure our success and build on lessons learned.

We thank you for your interest in the Government's development of Australia's 2020 Cyber Security Strategy and we look forward to receiving your views.

Call for views

You may wish to answer some or all of the following questions

1. What is your view of the cyber threat environment? What threats should Government be focusing on?
2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?
3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider?
4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?
5. How can Government maintain trust from the Australian community when using its cyber security capabilities?
6. What customer protections should apply to the security of cyber goods and services?
7. What role can Government and industry play in supporting the cyber security of consumers?
8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

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

10 Is the regulatory environment for cyber security appropriate? Why or why not?

11 What specific market incentives or regulatory changes should Government consider?

12 What needs to be done so that cyber security is 'built in' to digital goods and services?

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

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

15 Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

16 How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

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

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

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

20 What funding models should Government explore for any additional protections provided to the community?

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

22 To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

23 How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

24 What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

25 Would you like to see cyber security features prioritised in products and services?

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

Appendix A:

Progress against Australia's 2016 Cyber Security Strategy

1	**Action** Deliver progress updates on the implementation of this Strategy	**Assessment** Ongoing
	Notes The first update was published in 2017. This appendix is the second update on progress against the 2016 Strategy.	
2	**Action** Hold annual cyber security leaders' meetings	**Assessment** Ongoing
	Notes The former Prime Minister hosted two industry roundtables in 2017.	
3	**Action** Streamline the Government's cyber security governance and structures	**Assessment** Complete
	Notes The Australian Signals Directorate (ASD) has been established as a statutory agency and the Australian Government's cyber security functions are now co-located in ASD's Australian Cyber Security Centre (ACSC). An Ambassador for Cyber Affairs has been appointed.	
4	**Action** Sponsor research to better understand the cost of malicious cyber activity to the Australian economy	**Assessment** Updated Approach
	Notes This activity was overtaken by a classified review of the threat and vulnerability landscape in Australia.	

	Action	Assessment
5	In partnership with the private sector, establish a layered approach to cyber threat information sharing through: – partnerships between businesses and the government within the ACSC – co-designed joint cyber threat sharing centres in key capital cities – a co-designed online information sharing portal	Ongoing

Notes

Joint Cyber Security Centres (JCSCs) were established in Sydney, Brisbane, Melbourne, Perth and Adelaide. The ACSC has also been working with the Tasmanian and Northern Territory governments to provide further support to partners in those locations, including establishing video-conferencing facilities to enable local partners to participate in ACSC events.

The JCSCs have established strong collaborative programs with state and territory governments, academic institutions, and a wide range of key industry and small business associations.

The JCSCs have provided a national platform for the development and delivery of ACSC-wide programs, such as the electricity sector resilience work led by the National Exercise Program. The JCSC's established presence and network of relationships enables the ACSC to project its capability to a significantly expanded cross-section of the Australian economy.

An interim public-private communications platform has been established while a long term solution is created. And ASD continues to develop co-designed online information sharing portals within the cyber.gov.au platform.

	Action	Assessment
6	Increase the Computer Emergency Response Team (CERT) Australia's capacity within ACSC	Complete

Notes

CERT was absorbed into ASD as part of Machinery of Government changes which took effect in July 2018.

A 24/7 incident response capability has been established within ASD, expanding the services that CERT and ASD previously provided to businesses and government.

	Action	Assessment
7	Boost the Government's capacity to fight cybercrime in the Australian Criminal Intelligence Commission	Complete

Notes

The Australian Criminal Intelligence Commission (ACIC) now provides a criminal intelligence capability to the ACSC. The ACIC has improved understanding of Australia's cybercrime threat landscape by contributing to the ACSC's cyber threat reports and delivering themed intelligence assessments and insights. The ACIC has also expanded the Government's capacity to target criminals cashing out the proceeds of cybercrime in Australia; identified and deepened understanding of the top criminal and technical targets impacting Australia and its interests, and contributed to the ACSC cybercrime top 10 priority threat list; and worked with partners to develop alternative response and disruption measures to mitigate cybercriminal activity targeting Australia.

	Action	Assessment
8	Boost the Government's capacity to fight cybercrime in the Australian Federal Police	Complete

Notes

The Australian Federal Police (AFP) has strengthened our capacity to fight cybercrime by embedding additional sworn police investigators, technical specialists and intelligence analysts in the ACSC and in the dedicated AFP Cyber Teams. AFP's Cybercrime Operations currently comprises 69 positions, 25 of which are funded under the 2016 Cyber Security Strategy. This greatly enhanced the capacity to fight cybercrime by embedding additional sworn investigators, technical specialists and intelligence analysts who engage across multiple jurisdictions, conducting assessments, triaging, investigating and disrupting cybercrime.

The AFP has also conducted advanced investigator cyber training in all regions to enhance the base capabilities of general investigators. These increased capabilities are due to the increased Government investment in this crime type. Without this investment AFP will be unable to perform its role effectively as the Commonwealth's primary law enforcement agency or as a key pillar in the Government's cyber defences.

	Action	Assessment
9	Collaborate with Australian governments to ensure law enforcement officers receive the required training to fight cybercrime across the nation	Complete

Notes

The AFP has delivered cybercrime training to more than 650 participants from law enforcement, intelligence and cyber security agencies across Australia.

10	**Action** Increase ASD's capacity to identify new and emerging cyber threats to our security and improve intrusion analysis capabilities	**Assessment** Complete

Notes

In July 2018, ASD established a new Hunt and Trends Team responsible for:

- proactive discovery of previously unknown forms of adversary tradecraft and system compromises in priority Australian networks; and
- identification of trends in the scale and scope of malicious activity affecting Australia, to inform ASD's discovery, mitigation and disruption efforts.

11	**Action** Strengthen Defence's cyber security capacity and capability, through initiatives in the 2016 Defence White Paper	**Assessment** Complete

Notes

The Department of Defence established an Information Warfare Division in July 2017 as part of the Defence White Paper.

12	**Action** Expand the nation's cyber incident management arrangements and exercising program	**Assessment** Complete

Notes

National Cyber Incident Management Arrangements were agreed by the Council of Australian Governments in December 2018.

For the 2018–19 Financial Year, the ACSC National Exercise Program has supported 55 cyber security exercise activities with Federal, state and territory governments, international governments, and owners and operators of Australia's critical infrastructure.

13	**Action** Co-design voluntary guidelines on good cyber security practice	**Assessment** Complete

Notes

ACSC provides a range of voluntary guidance products. For example, in response to the global compromise of Managed Service Providers as part of the Cloud Hopper operation, the ACSC has launched guidance on best practices for Managed Service Providers. This was co-designed with trusted industry partners.

14	**Action** Continue to regularly update ASD's Strategies to Mitigate Targeted Cyber Intrusions	**Assessment** Complete
	Notes This advice is now called the *Strategies to Mitigate Cyber Security Incidents*, including the 'Essential Eight' mitigation strategies, and is complemented by the *Essential Eight Maturity Model* which was most recently updated in July 2019.	
15	**Action** Co-design voluntary cyber security 'health checks' for ASX100 listed businesses	**Assessment** Complete
	Notes Health checks have been completed and the report was published in April 2017.	
16	**Action** Support the Council of Registered Ethical Security Testers (CREST) Australia New Zealand to expand its range of cyber security services	**Assessment** Complete
	Notes CREST has expanded its services, and developed the Small Business Cyber Security Health Check. The service is designed to assist small businesses in understanding their cyber security maturity.	
17	**Action** Support small businesses to have their cyber security tested by CREST Australia New Zealand accredited providers	**Assessment** Complete
	Notes The Cyber Security Small Business Program was launched in December 2018. Businesses with 19 or fewer employees can receive a co-funded grant of up to $2,100 for a certified small business cyber security health check to determine business risk and areas that need attention.	

18	**Action** Improve Government agencies' cyber security through a rolling program of independent assessments of agencies' implementation of ASD's Strategies to Mitigate Targeted Cyber Intrusions	**Assessment** Updated approach

Notes

ASD is using new technology solutions to improve agency cyber hygiene at scale. This includes automated scanning tools to identify vulnerabilities in external facing systems across government.

Dedicated technical 'Sprint Teams' have also been created to uplift cyber security for select Australian Government agencies. In addition to improving cyber hygiene these Sprint Teams will create a situational awareness of the maturity across these agencies of their implementation of the Essential Eight Maturity Model.

19	**Action** Improve Government agencies' cyber security through independent cyber security assessments for agencies at higher risk of malicious cyber activity that also helps those agencies address the findings	**Assessment** Updated approach

Notes

ASD has conducted active vulnerability assessments of a number of key government agencies and provided clear guidance on mitigation and network improvement.

20	**Action** Improve Government agencies' cyber security through increasing the Australian Signals Directorate's capacity to assess Government agencies' vulnerability, provide technical security advice and investigate emerging technologies	**Assessment** Complete

Notes

ASD continues to improve its capacity to deliver cyber security advice and assistance across Government. In the last 12 months this has included:

- actioning over 600 individual service requests across Government since July 2017
- providing a number of Government agencies with a range of prototype security validation tools
- regularly updating the Information Security Manual and Essential Eight Maturity Model to ensure ASD provides the most relevant and applicable technical security advice
- establishing a dedicated section focused on investigating emerging technology and providing advice and guidance to Government
- launching the Critical Infrastructure Lab, which is being used to raise awareness of critical infrastructure security issues and research best practice in system configuration
- launching the Internet of Things (IoT) Lab to enable investigation of IoT product security and respond to incidents.

21	**Action** Develop guidance for Government agencies to consistently manage supply chain security risks for ICT equipment and services	**Assessment** Complete

Notes

ASD developed, in consultation with industry and government stakeholders, a technical guidance on cyber supply chain risk management for practitioners and executives. This guidance was published on cyber.gov.au on 25 June 2019.

The Government-issued guidance provided in August 2018 to network providers highlighted the security risks that arise in 5G networks. As of 18 September 2018, the *Telecommunications Act 1997* requires network operators to protect Australian communications from unauthorised interference or access that might prejudice Australia's national security.

22	**Action** Appoint a Cyber Ambassador	**Assessment** Complete

Notes

Tobias Feakin was Australia's inaugural Ambassador for Cyber Affairs.

23	**Action** Publish an international engagement strategy on cyber security	**Assessment** Complete

Notes

Australia's International Cyber Engagement Strategy was published in October 2017. The Foreign Minister released a publicly available progress report in March 2019.

24	**Action** Champion an open, free and secure internet to enable all countries to generate growth and opportunity online	**Assessment** Complete

Notes

Australia champions an open, free and secure internet in a range of international forums, bilaterally and in multilateral groups including the UN, East Asia Summit and ASEAN Regional Forum. Australia has partnered with countries in the region through cyber policy dialogues to advance our advocacy of an open, free and secure cyberspace. Australia has worked with international partners to secure leader-level re-affirmation of key tenets of international stability in cyberspace including the application of existing international law and agreed norms of behaviour.

25	**Action** Partner internationally to shut down safe havens and prevent malicious cyber activity, with a particular focus on the Indo-Pacific region	**Assessment** Ongoing
	Notes Australia has presented at and contributed to a range of regional cybercrime workshops.	
26	**Action** Build cyber capacity in the Indo-Pacific region and globally, including through public-private partnerships	**Assessment** Complete
	Notes Australia will invest nearly $34 million out to 2023 to strengthen cyber capacity and resilience in the Indo-Pacific region. This includes Australia's Cyber Cooperation Program which has expanded from $4 million to $34 million over four years, and $14.4 million for a sustained cyber security partnership with Papua New Guinea for the Asia-Pacific Economic Cooperation (APEC) and beyond.	
27	**Action** Establish a Cyber Security Growth Network to bring together a national cyber security innovation network that pioneers cutting edge cyber security research and innovation, through the National Innovation and Science Agenda	**Assessment** Complete
	Notes AustCyber was established in late 2016, and operational from 1 January 2017. AustCyber's mission is: to support the development of a vibrant and globally competitive Australian cyber security sector, thus enhancing Australia's future economic growth in a digitally enabled global economy.	

28	**Action** Boost Data61's capacity for cyber security research, support to commercialisation of cyber security solutions, improving cyber security skills and deepening connections with international partners, through the National Innovation and Science Agenda	**Assessment** Complete

Notes

CSIRO's Data61 has boosted its capacity by implementing a cyber security strategy and providing commercialisation support with a focus on trustworthy systems, risk-based cyber approaches, secure data sharing and the human dimension of cyber security. This includes a three year research partnership with Defence Science and Technology Group and other partners, which involves 23 joint research projects, delivered in collaboration with 15 universities.

29	**Action** Work with business and the research community to better target cyber security research to Australia's cyber security challenges	**Assessment** Complete

Notes

The Cyber Security Cooperative Research Centre (Cyber Security CRC) has been established to support and enable collaboration and co-development across Australia's cyber security ecosystem. The Cyber Security CRC has leveraged $84.4 million worth of contributions from 25 industry, state government, university and research participants, in addition to $50 million from the Australian Government over seven years, totalling $134.4 million.

30	**Action** Promote Australian cyber security products and services for development and export	**Assessment** Complete

Notes

Initiatives such as AustCyber working with Austrade's Landing Pad Program and other partners have helped Australia's world class cyber security industry capitalise on new commercial opportunities. With AustCyber, over 100 Australian companies have travelled to the US, UK, Singapore, Israel, India and the Association of Southeast Asian Nations (ASEAN) across eight trade delegations to engage with global partners and customers.

31	**Action**	**Assessment**
	Partner with Australian governments, businesses, education providers and the research community in a national effort to develop cyber security skills – establish academic centres of cyber security excellence in universities – introduce programs for all people at all levels in the workforce to improve their cyber security skills and knowledge, starting with those in executive-level positions – continue to raise awareness in schools of the core skills needed for a career in cyber security – understand and address the causes of low participation by women in cyber security careers – expand the Government's annual Cyber Security Challenge Australia to a broader program of competitions and skills development	Ongoing

Notes

Academic Centres of Cyber Security Excellence have been established at Edith Cowan University (ECU) and the University of Melbourne.

AustCyber designed and is implementing a series of cyber security challenges developing technical and non-technical skills for Australians across all age groups. These challenges are being delivered through a range of partnerships with industry and academia.

Annual Women in Cyber Mentoring Events, held across Australia, are bringing together female students with successful women in the industry. These cyber professionals are at varying stages of their careers, and serve as role models, offering a 12-month program of mentorship and guidance.

The Cyber Security Challenge Australia event was scaled up, resulting in 450 per cent growth in participation from TAFEs and over 50 per cent increase in student participation overall in 2018. ASD is reviewing the Challenge requirements for future years.

32	**Action**	**Assessment**
	Bring together and grow public and private sector cyber security awareness programs to make the best use of combined resources	Complete

Notes

ASD coordinates awareness-raising about online security by the Australian Government through a stakeholder group of over 20 Australian Government agencies. This group shares information, collaborates and amplifies the awareness-raising activities of agencies, such as the ASD's Stay Smart Online program, the Australian Competition and Consumer Commission's Scamwatch, Office of the Australian Information Commissioner, Office of the eSafety Commissioner, Australian Taxation Office, Digital Health Agency and the Department of Human Services.

ASD and other Australian Government agencies also work with a range of industry partners and the Security, Influence and Trust Group to grow public and private sector awareness programs.

The Stay Smart Online program, which provides easy-to-understand online security advice to individuals and small/medium businesses has grown its community 20 per cent each year, and has over 1500 partners from industry, education and government sectors that share advice and information with their employees and customers. The annual national awareness-raising week, Stay Smart Online Week, has reached about 3 million Australians each year, in the last two years.

33	**Action**	**Assessment**
	Work with other countries on cyber security awareness raising programs to deliver mutually beneficial outcomes	Complete

Notes

ASD routinely engages with international counterparts in the development of awareness raising programs. For example, following the attribution of the global compromise of managed service providers, ASD coordinated advice and guidance for industry with international partners to achieve maximum reach and impact.

Australian Government