EY's view to Australia's 2020 Cyber Security Strategy

Australian Government

6 November 2019

Building a better working world

Building a better working world

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

Greg Miller
First Assistant Secretary
Cyber Security Policy
Department of Home Affairs
6 Chan Street
Belconnen ACT 2617

6 November 2019

EY's view to Australia's 2020 Cyber Security Strategy

Dear Greg,

On behalf of Ernst & Young (EY), I would like to thank you for the opportunity to present our view to Australia's 2020 Cyber Security Strategy.

We understand the drivers and importance for the Department of Home Affairs to develop Australia's next Cyber Security Strategy as part of its commitment to protecting Australians from cyber security threats.

We understand the cyber threat environment in Australia is not isolated from the same disruptors as seen across the world in Government, industry and broader communities, where cyber security trends indicate a breach is increasingly a matter of "when, not if", and preventive controls are no longer enough. We also understand the Australian community entrust the Government, with increasing amounts of their most sensitive and critical data.

The process of preparing this document took a concerted effort across EY's national cyber security team to attend and participate at the Departments' workshops held over the past 7 weeks in each of the cities. It was important for us to show a presence at those workshops and to share our individual points of view in the breakout sessions. This active presence combined with numerous internal workshops that brainstormed, contested and consolidated opinions which ultimately formed the foundation of this document. EY's combination of extensive experience in providing cyber security transformation programs and services, as well as our experience across private and public sectors, both in Australia and globally, will provide you with uniquely positioned views to Australia's 2020 Cyber Security Strategy.

Yours sincerely,

[redacted]

Glen Gooding
Partner, Cyber Security

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

EY's views on Australia's 2020 Cyber Security Strategy

Where we are now

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

The cyber threat environment in Australia is not isolated from the same disruptors as seen across the world in Government, industry and broader communities. We continue to lose the race to cyber attackers who have the tools, time and persistence to exploit zero-day-vulnerabilities even before a patch is released. The rise of state-sponsored and geo-targeting cyber-attacks, the use of cryptocurrency to fund eCrime and hacktivism, and evolving threats like ransomware are all part of the adversary to stay ahead of hackers. Moreover, cloud computing, borderless data and increased adoption of automation and technologies such as Industrial Internet of Things (IIoT) are key examples of the move to wide-adoption of new technology without completely understanding the threats that accompany.

Threats the Government should be focusing on include:

- State-sponsored threats, such as the likely state-sponsored attack of Australian Parliament in February 2019, continue to be a growing threat for Government and critical infrastructure industry-alike.
- Organised eCrime and hacktivism, such as online fraud and hacking, cost the Australian economy up to $1 billion annually in direct costs. The Australian Government is an attractive target of serious and organised crime syndicate due to the nature of the information the Government holds.
- Security of IIoT, such as interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management. Due to a greater exposed attack surface, Operational Technologies (OT) introduce significant security risks within manufacturing, utility, liquid fuel and other critical infrastructure groups.
- Cryptojacking, known as "Cryptomining malware", uses both invasive methods of initial access, and drive-by scripts on websites, to steal resources from endpoints, mobile devices, and servers. This type of attack runs quietly at the background which makes it difficult to detect and remove.

Positioning ourselves for the future

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

The responsibility of managing cyber security risks should be a consideration for the Australian Government, industry and the broader Australian community. End-users, such as individuals and small business and providers of goods and services should continue to be responsible for managing cyber security risks within their own supply chains.

However, these end users should also continue to engage within their respective industries and across other like-industries to share information on new and emerging cyber security risks.

The value of data continues to increase. Amazon, Apple, Google, Microsoft and Facebook are some of the world's most valuable brands that host data on Australian shores. The Australian Government and industry alike should consider additional regulation and controls over data privacy and security.

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

Federal, state and territory government's roles should expand from not only protecting government networks, enforcing the law and offering security advice but to also provide a standardised approach to cyber security and its associated regulatory environment. The concept of a standardised approach is explained further in question 10.

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

As mentioned in question 2, the Australian Government should consider additional regulation and control over data privacy and security, ultimately to appropriately manage cyber security risks in the economy. Controls such as a centralised threat information sharing platform in conjunction with a standardised approach to cyber security and its associated regulatory environment will see an increase in cyber security defence posture.

Minimal information sharing between the Australian Government, industry and broader Australian Community increases the risk of an uncoordinated response in the event of a coordinated cyber incident or attack. The Australian Government, in conjunction with industry need to develop consistent cyber security standards and communication channels.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) for example is a dedicated forum for business, trade and commerce to reduce cyber security risk in the global financial system.[1] Forums such as the FS-ISAC will support cyber security information sharing across the Australian Government, industry and broader Australian Community.

Eliminating the ambiguity in the three lines of defense for cyber security and adding the government as the fourth line of defense we believe is required to correctly address and mitigate cyber security risks.

Government's role in a changing world

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

The Australian Government should work with other Government Agencies, security institutions, risk managers, cyber security practitioners and the private sector to address the most serious cyber security threats.

The Australian Government's role should be to make sure, in response to the most serious threats, the right people, skills, equipment and resources are available. Second to that and by far the most critical investment by the Government should be in relation to the education of Australian citizens on the cyber security risks that affect them personally as well as their business. The aim is to create a shift from the passive participation to proactive and collective change to the Australian security maturity baseline. This in turn ensures that more institutions and local businesses are investing into cyber skills, equipment and resources and therefore the burden to protect Australia is not on the government alone.

Furthermore, the Australian Government provides the governance to a response, that in-turn will define a national response. The Australian Government should have an ability to mobilise a community of subject matter resources from across Government, security institutions and the private sector in addressing the most serious threats.

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

To maintain trust from the Australian community when using its cyber security capabilities, the Australian Government should ensure transparency throughout its cyber security capability lifecycle–from identifying, detecting and responding to a cyber-attack, all the way through to producing post-cyber-attack reports or updates.

Post-cyber-attack reports, Indicator of Compromise (IoC) or updates should include at a minimum:

[1] https://www.fsisac.com/who-we-are

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

- What the cyber-attack was
- What the impact was
- The actions made by the Australian Government
- The result of the cyber-attack, including actions made to recover and lessons learned to prevent and/or mitigate similar incidents or attacks in the future

Enterprise, innovation and cyber security

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

The security of cyber goods and services should be in a consumer-friendly system, which will provide consumers with assurance over goods and services.

For example, applying a similar concept to the Common Criteria for Information Security Evaluation (Common Criteria)[2] will contribute to the security of cyber goods and services. Participants of Common Criteria arrangements share the following objectives:

- Ensure evaluations of Information Technology (IT) products and protection profiles are performed to a high and consistent standard and are seen to contribute significantly to confidence in the security of products and profiles.
- Improve the availability of evaluated, security-enhanced IT products and protection profiles.
- Eliminate the burden of duplicating evaluations of IT products and protection profiles.
- Continuously improve the efficiency and cost-effectiveness of the evaluation and certification/ process for IT products and protection profiles.[3]

Ultimately, Common Criteria enables an objective evaluation to validate that a product or system satisfies a defined set of security requirements.

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

The Australian Government and industry have a large role in supporting cyber security of consumers.

Australian and industry should consolidate and expand existing cyber security awareness campaigns and programs to support Australian consumers. Existing cyber security awareness campaigns and programs with opportunities for consolidation and expansion include the following:

- The **Stay Smart Online Program** as delivered by the Australian Cyber Security Centre currently provides topical, relevant and timely information on how home internet users and small business can protect themselves from, and reduce the risk of, cyber security threats. The Stay Smart Online Program involves a community of more than 80,000 individuals and organisations.[4]
- The **Australian Internet Security Initiative**, also run by the Australian Cyber Security Centre helps reduce malicious software infections and services vulnerabilities occurring on Australian internet protocol address ranges.[5]
- The **Joint Cyber Security Centres** which bring together business, research community with state, territory and Federal Government in an open and cooperative environment.[6]

The Australian Government and industry can combine alerts, bulletins (with how to guides) and advisor services. By consolidating and expanding existing cyber security awareness campaigns, the Australian Government and industry can support a standardised approach to cyber security.

[2] https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria
[3] https://www.commoncriteriaportal.org/ccra/index.cfm
[4] https://www.staysmartonline.gov.au/about-us
[5] https://portal.aisi.gov.au/
[6] https://www.cyber.gov.au/index.php/programs/joint-cyber-security-centres

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

For example, the Cyber Security and Infrastructure Security Agency (CISA) is the United States' risk advisor. CISA provides the United States (US) Government, industry and community extensive cyber security and infrastructure security knowledge and practices, shares knowledge to enable better risk management and puts it into practice to protect the US's most essential resources. CISA has established a National Cyber Awareness System (NCAS) that provides various informational products across both technical and non-technical cyber security issues. The informational products include subscriptions to:

- Current Activity entries that provide up-to-date information about high-impact types of security activity affecting the US Government, industry and broader community.
- Alerts that provide timely information about new and emerging security issues, vulnerabilities, and exploits.
- Bulletins that provide weekly summaries of new vulnerabilities and associated patch information.
- Tips that provide advice about common security issues for the broader US community.
- Industrial Control System Alerts that provide timely notification to critical infrastructure owners and operating concerning threats or activity with the potential to impact critical infrastructure computing networks.
- Industrial Control Systems Advisories that provide timely information about new and emerging industrial control systems (ICS) security issues, vulnerabilities and exploits.[7]

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

Under a shared responsibility model, the Australian Government and industry can sensibly increase the security, quality and effectiveness of cyber security and digital offerings.

An example of a shared responsibility model is the one used between Amazon Web Services (AWS) and their customers. Under this model AWS is responsible for "Security of the Cloud" and Customers are responsible for "Security in the Cloud". A model such as this could see:

- Government responsible for the regulatory environment for cyber security and digital offerings
- Industry be responsible for security, quality and effectiveness of cyber security and digital offerings
- Consumers be responsible for being cyber security aware

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

The Australian Government and industry should work together to break down boundaries to promote greater information sharing.

While some cyber security threat information the Australian Government collects is classified for national security purposes, the Australian Government should consider what information could be shared with industry. Industry equally, may maintain cyber security threat information that could be shared amongst other industries and to Australian Government.

As previously discussed in question 3, increased information sharing will see an increase in Australia's cyber security defence posture. As discussed in question 7, the Australian Government needs to consolidate and expand existing cyber security awareness campaigns and programs. To expand existing cyber security awareness campaigns could involve the roles and responsibilities of industry partners of the Stay Smart Online Program to expand messages and awareness of cyber security.

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

Innovation in many sectors is occurring faster than ever before, this means that for many industries it's no longer a question if new technologies should be taken up but rather how fast they can be implemented. In

[7] https://www.us-cert.gov/about-us

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

some sectors that innovation means early detection of diseases or lifesaving treatment, where at face value the benefits far outweigh the risk. Combine that with a need to live in a more connected world cyber security risks become exponentially more difficult to manage.

All over the world we are only just playing catch up to the cyber security risks that that are well known to us. Our current regulatory environment is working at managing the known issues such as data protection through our Data Privacy Legislation. However, Government agencies need to continue to combine their efforts and focus on the future state.

As an example, the CSIRO should develop the bare minimum-security requirements that innovators need to consider when building medical devices. In line with our response in question 1 the future of the IIoT needs to be defined and as such minimum-security requirements need to be included.

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

Answer to questions 10 & 11: There are opportunities to standardise the approach to cyber security and its associated regulatory environment in Australia-across government and industry. While there is no overarching cyber security framework or standard which is either recommended or mandated by the Australian Government, the Australian Government's Information Security Manual (ISM) is available for industry to apply, in conjunction with their own risk management frameworks to protect information and systems from cyber security threats. However, is not widely used beyond Government.

For example, the US Department of Homeland Security (DHS) works with key partners across Federal, state and local government, industry, and the international community to identify and manage national cyber security risks. The DHS Cyber Security Strategy sets out five pillars of a DHS-wide risk management approach and provides a framework for executing cyber security responsibilities and leveraging the full range of DHS's capabilities to improve cyber security resilience. The five pillars are:

- Risk Identification
- Vulnerability Reduction
- Threat Reduction
- Consequence Mitigation
- Enable Cyber Security Outcomes[8]

The risk of a lack of a standardised approach to cyber security and its associated regulatory environment in Australia limits Government, industry and by extension, the Australian Community to understand cyber security and its ability to build a resilient, cyber-aware country. A standardised approach provides strategic direction, identifying what mature risk and control environments look like.

Further, a standardised approach to cyber security will assist Government to provide an appropriate level of regulation to

- Underpin Australia's cyber security strategy
- Protect the rights and safety of citizens
- Provide a business approved level of Confidentiality, Integrity and Availability of digital goods and services.

A trusted marketplace with skilled professionals

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

Trust by Design – is an EY methodology that has revolutionised risk by instilling a risk optimisation mind-set which embedded trust into services and products from the outset. By adopting a Trust by Design

[8] https://www.dhs.gov/news/2018/05/15/fact-sheet-dhs-cybersecurity-policy

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

approach to cyber security, the Australian Government will be able to provide confidence and trust into digital goods and services. The Australian Government in conjunction with industry should consider how:

- Cyber security can help balance opportunities with threats, while also providing opportunity to monitor what's going on externally to help address any issues that arise, and
- Embracing cyber security will act as an enabler of trust and confidence.[9]

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

The Australian Government should consider a regulated approach to instilling better trust in ICT supply chains.

A good example is the Financial Services Sector to see how standards and due diligence over cyber security capability and maturity can instill better trust in ICT supply chains. Where organisations are expected to achieve a minimum baseline of security for the management of data in ICT supply chains the collective trust in ICT supply chains is increased. For example, the Australian Prudential Regulation Authority's (APRA) CPS 234 Information Security prudential standard requires that where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity.[10]

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

Federal, state and local governments need to work in conjunction with private entities to build a market of high-quality cyber security professionals in Australia. Growth of newly skilled cyber professionals needs to start as early in the educational lifecycle as possible. The Australian Government should consider:

- Expanding cyber security education campaigns in existing cyber security programs such as the Australian Cyber Security Growth Network.[11]
- Developing cyber security curriculum for use in Australian primary and high schools.
- Implementing a scholarship program for vocational and tertiary level students seeking a career in cyber security. The Australian Government has seen great success from the New Colombo Plan initiative to lift knowledge of the Indo Pacific in Australia by supporting Australian undergraduates to study undertake internships in the region.[12]
- Once a cyber aware, workforce student is ready for industry, it is the private sectors role to move away from traditional tertiary qualification entrance criteria and look to the skillsets of the individual and not their degree.

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

The key barrier preventing the growth of the cyber insurance market in Australia is a lack of a standardised approach to cyber security.

Without a lack of a standardised approach to cyber security, there is a lack of a baseline model for organisations to understand what "good" looks like. A standardised approach to cyber security that includes a baseline of controls and/or maturity levels will enable the growth of the cyber insurance market in Australia.

A hostile environment for malicious cyber actors

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

[9] https://www.ey.com/en_gl/trust-by-design
[10] https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
[11] https://www.austcyber.com/about-us
[12] https://dfat.gov.au/people-to-people/new-colombo-plan/pages/new-colombo-plan.aspx

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

With the implementation of a standardised approach to cyber security, which considers Defence in Depth, high-volume, low-sophistication malicious activity targeting Australia will be reduced.

Defence in Depth is the concept of protecting a computer network with a series of defensive mechanisms such that is one mechanism fails, another will be in place to thwart an attack. By considering a Defence in Depth approach to cyber security, you are increasing adversarial cost.[13]

The Australian Government or related security agencies might consider joint investment with telecommunication carriers and media distribution hubs to invest in protection through detection which is subsidised if developed and sourced locally to promote further investment and growth of capability in the industry.

Further, a cyber border control mechanism utilising detection technologies and intelligence network feeds to identify the gaps in environment and shape the future of cyber security strategy.

Lastly, an increase in the end-user awareness through nation wide campaigns to educate the citizens from all age groups and backgrounds on online-safety. This can be done through initiatives like the eSafety Commissioner, the independent statutory office supported by the Australian Communications and Media Authority helping Australians to have safer, more positive experiences online.[14]

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

The best method to thwart an attack is to redirect it and slow it down, hence we suggest there be a strategy to engineer methods of deception, delay and, detection.

Why we don't recommend the use of honey pots? Honey pots are expensive and difficult to maintain, while deception is a reasonably cost-effective method of slowing threat actors down. Deception methods that do not require a honey pot environment can also be used to proactively flush out hackers and leakers.

A bad threat actor will generally act anonymously and rely on various tools for anonymity. These tools often contribute to the success of their various attacks and methods. Deception techniques can be used to reveal attackers, often without their knowledge. This provides a potential route for law enforcement to hold hackers and leakers accountable.

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

Refer to the response for question 19.

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

Answer to questions 18 & 19: With the implementation of a standardised approach to cyber security, the Australian Government can also implement a cyber security risk management framework that identifies critical Information and Communications Technology (ICT) infrastructure based on a risk-management approach.

Based on risk, the Australian Government and private entities can appropriately identify controls to mitigate identified risk. A standardised approach to cyber security in conjunction with defined controls will enable the Australian Government and private entities to better proactively identify and remediate cyber security risks.

Private networks that should be considered critical systems that require stronger cyber defence systems include networks that reside in health and education sectors.

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

The Australian Government should explore:

[13] https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525
[14] https://www.esafety.gov.au/about-us

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

- Expanding cyber security grants across industry for small and large businesses for cyber security capability and maturity uplift.
- Providing further support to organisations, such as the Australian Federal Police, Australian Cyber Security Centre and the Australian Secret Intelligence Organisation that contribute to combating complex, transnational, cybercrime. In a review by the Department of Prime Minister and Cabinet, cybercrime is costing the Australian economy up to $1 billion annually in direct costs alone.[15]

Moreover, the SME community is highly vulnerable to ransomware attacks and other threat vectors, purely due to their size and lack of IT and cyber security budget. A funding model, let's call it "CyberBasics", to get the foundational aspects of cyber security implemented within their organisations is recommended. This could lead to ongoing 'business owner' awareness sessions (could even be accreditation) that SME owners are sufficiently protected.

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

Constraints to information sharing between Government and industry on cyber threats and vulnerabilities include a lack of established secure information sharing platforms in conjunction with a standardised approach to cyber security and its associated regulatory environment. Other constraints to information sharing include:

- The National Security Information (Criminal and Civil Proceedings) Act 2004
- Intellectual Property and competitive advantage

To enhance the ability to jointly respond to cyber incidents the Australian government could consider a Consortium approach to Cyber Managed Services which includes Carriers, Financial Institutions, Industry, Tertiary Education and local governments. This would allow an "Open" community-based approach through a trusted service provider framework which enables intelligence sharing, increased bargaining power and standardised operations. Indicators of Compromise (IoC), threat intelligence and active actors presented at a point in time need to be shared. No Intellectual Property (IP) or Personally Identifiable Information (PII) data should be shared across any group of organisations looking to defend against outside threats.

A cyber-aware community

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

A lack of cyber security awareness to a large extent drives poor consumer choices and/or market offerings.

A lack of cyber security awareness increases the risk that individuals are no longer able to own their data and digital identity online. The Australian Government and industry need to provide education on online behaviours. For example, when you enter agreements to use an application you are also agreeing to share certain information and/or data. At a minimum, individuals need a baseline understanding of:

- The value of the information and/or data they hold
- What information and/or data is being requested
- Where and how information and/or data is being stored

Strengthened cyber security awareness campaigns will give an individual the power to share or not share their information.

A further enhancement to any awareness campaign is providing a high level of visibility.

[15] https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

Visibility can be demonstrated as a Cyber Security Dashboard Risk Reporting (akin to a weather map) – providing unified visualisations to monitor and measure the security posture, health and risk of the current ICT environment by industry.

The metrics for reporting would be jointly defined by the Australian Government and industry bodies.

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

An increased consumer focus on cyber security will benefit Australian business who create cyber secure products because consumers will be more inclined, when presented with a choice, to trust an established and trusted business.

A Cyber stamp of approval, akin to a "100% Australian Made" stamp of approval would encourage buyers of new products to invest in technology that has a cyber by design built into their products.

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

Examples of best practice behaviour change campaigns or measures include:

- **Stay Smart Online Week** as part of the Stay Smart Online Program run by the Australian Government has demonstrated the strength of the relationships between the Australian Government with other governments, industry, business and individuals. By establishing a community that encourages business to share experiences and best practice it empowers others to learn to better protect information.

- The **Stop Think Connect** campaign brought together a coalition of private, non-profit and government organisations in partnership with the government in the US.[16] The campaign was chosen by a coalition of organisations and government due to the extensive research and surveys performed for cyber security awareness, which revealed that Individuals are concerned about their personal security, safety and privacy. The research, which consisted of focus groups, opinion polling and government-industry collaboration also showed that consumers are ready to learn about the range of cyber security related topics and seek positive reinforcement that they can personally manage their own online safety.[17]

- The **Slip! Slop! Slap! SunSmart Campaign** was one of Australia's most successful health campaigns which has been recognised internationally since 1981. Utilising a carton with a catchy singing jingle on Australia's TV screens[18], the campaign has seen skin cancer rates reduce – a long-term study of teenagers and young adults has revealed the cases of melanoma in young people has fallen 5% each year from the mid-1990s to 2010.[19]

- The various **Anti-Drink Driving** campaigns delivered at state government levels. For example, Transport for NSW has engaged the community to help change unsafe behaviour on the roads through numerous campaigns including its **Plan B** campaign which began in 2012 campaigning for making positive choices to get home safely after a night out. The campaign has heavy emphasis on digital, cinema and television platforms with supporting advertisement on buses, taxis, and in licensed venues, where people are making the critical decision about whether to drink and drive. Since the campaign's inception, more than 80% of those surveyed recalled seeing the campaign and almost all supported it. Further, evaluations also found more than two thirds of the target audience agree that drinking and driving is not socially acceptable.[20]

Older generations will also need to be considered in future cyber security change campaigns as they are the group most at risk of not understanding cyber security, and therefore are targets for cyber criminals. Younger generations, while more aware than older generations, there is also a need to educate younger generations of maintains cyber security, especially privacy online.

[16] https://www.stopthinkconnect.org/about
[17] https://www.stopthinkconnect.org/research-surveys
[18] https://www.sunsmart.com.au/tools/videos/past-tv-campaigns/slip-slop-slap-original-sunsmart-campaign.html
[19] https://melanomaresearchvic.com.au/slip-slop-slap-success-skin-cancer-rates-plummet-thanks-long-running-nationwide-sun-safety-campaign
[20] https://roadsafety.transport.nsw.gov.au/campaigns/planb.html

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

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

A prioritisation of cyber security features in products and services will see an increase in consumer trust both within industry and by extension, for the Australian Government.

A Trust-by-Design approach needs to be factored in every technology product and service. By not implementing applicable security controls allows nation states and criminal organisations to further prioritise their target on Australian businesses. Where a standardised approach to cyber security that includes a baseline of controls and/or maturity has been implemented it will be easier for business to ensure cyber security features are not only prioritised but built-in to products and services.

Other Issues

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

The Australian Government should lead by example. If the Australian Government is spending money on its defences and implementing cyber security controls across federal, state and local governments it will make for a better business case in industry. If government recommended or mandatory controls are too hard to implement across government then it will be much harder to motivate action for increased cyber security capability and maturity in industry.

Ernst & Young
200 George Street
Sydney NSW 2000 Australia
GPO Box 2646 Sydney NSW 2001

Tel: +61 2 9248 5555
Fax: +61 2 9248 5959
ey.com/au

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business having the right advisors on your side can make all the difference. Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

Ernst & Young
A member firm of Ernst & Young Global Limited
Liability limited by a scheme approved under Professional Standards Legislation

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

Australian Auditing Standards have been issued by the Australian Auditing and Assurance Standards Board under s 336 of the Corporations Act 2001.

As the services covered by this project are not being performed under the requirements of the Corporations Act, the services do not constitute an external audit, or an engagement to perform agreed-upon procedures in accordance with the Australian Auditing Standards.

The services are being undertaken at the request of the Department of Home Affairs to examine the adequacy of internal controls outlined in the scope and approach sections of this document.

The Department of Home Affairs is fully and solely responsible for making implementation decisions, if any, and to determine further course of action with respect to any matters addressed in any advice, recommendations, services, reports or other work product or deliverables provided by us.

The Department of Home Affairs is responsible for maintaining an effective internal control structure. The purpose of our report will be to assist the Department of Home Affairs in discharging this obligation.

Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected. Further, the internal control structure, within which the control procedures that have been subject to internal audit operate, has not been reviewed in its entirety and, therefore, no opinion or view is expressed as to its effectiveness of the greater internal control structure. Any projection of the evaluation of control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

Our submission will be prepared for the use of the Department of Home Affairs. We disclaim all liability to any other third party for all costs, loss, damage and liability that the other third party may suffer or incur arising from or relating to or in any way connected with the contents of our report, the provision of our report to the other third party or the reliance upon our report by the other third party including your external auditor. We understand that whilst our work does not negate the primary obligations of your external auditor, the work we undertake may be accessed by the external auditor for their information only. Any reliance on our report will require separate consent by EY, The Department of Home Affairs and your external auditor.

ey.com