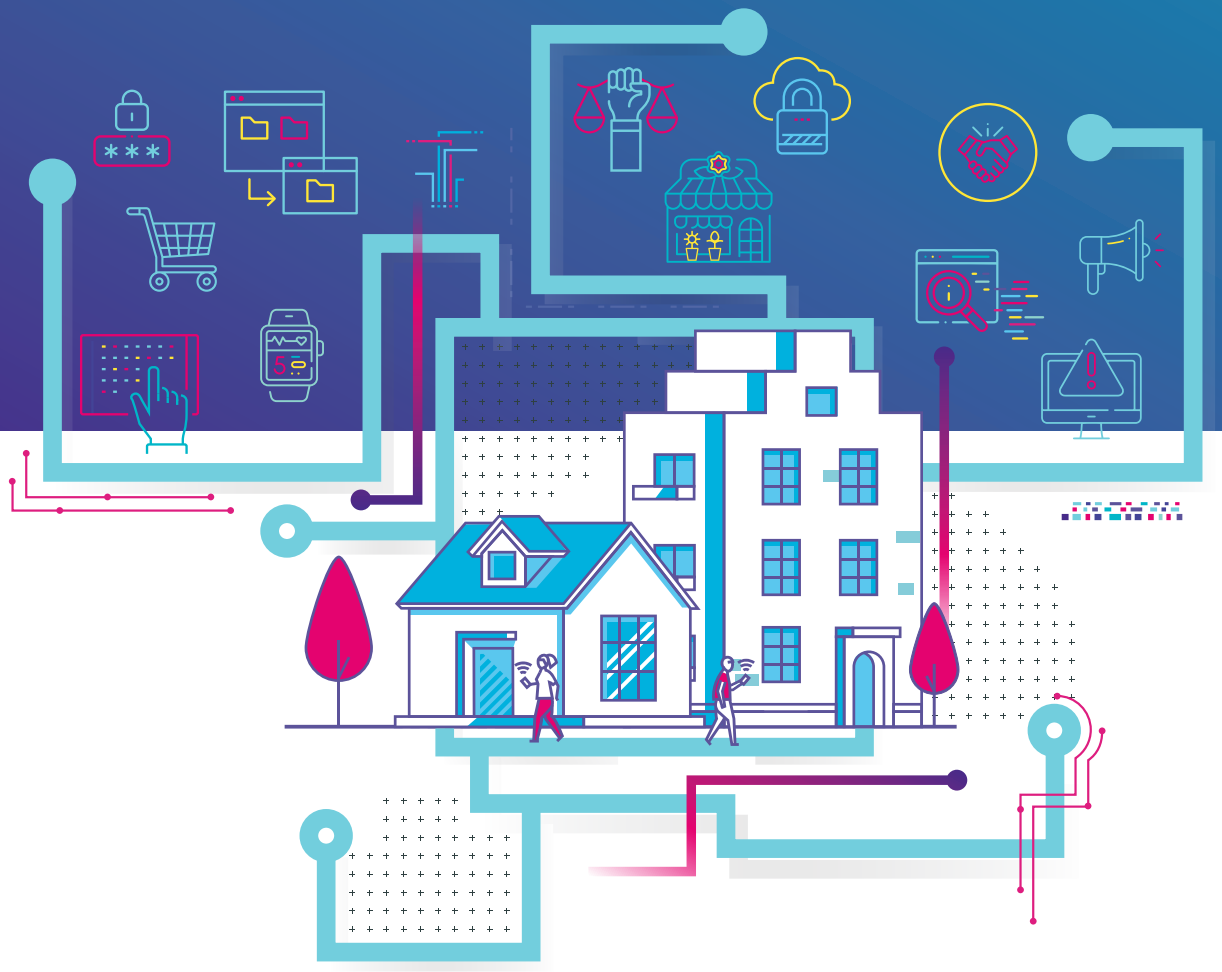
Australian Government

Strengthening Australia's cyber security regulations and incentives

An initiative of Australia's Cyber Security Strategy 2020



Quick summary

Executive Summary

A growing digital economy offers significant opportunities for all Australians, whether through new jobs, new business ventures or better ways to connect with each other. The COVID-19 pandemic has accelerated our transition to a digital economy and demonstrated the importance of the internet for our prosperity. However, as we become more connected, there are growing opportunities for cyber criminals to target Australians. It's clear that government, businesses and the community need to take steps to protect Australia from cyber security, privacy and online safety threats.

The discussion paper, *Strengthening Australia's cyber security regulations and incentives*, seeks your views about how the Australian Government can incentivise businesses to invest in cyber security, including through possible regulatory changes. This work is an initiative of *Australia's Cyber Security Strategy 2020* (the Cyber Security Strategy) and progresses recommendations of the 2020 Cyber Security Strategy Industry Advisory Panel. It will build on the Government's security of critical infrastructure reforms[1] by uplifting the cyber security of all digitally enabled businesses, and will ultimately support the Government's goal of being a leading digital economy by 2030.

This document provides a quick summary of the full discussion paper. As outlined in the quick overview below, we are proposing three areas of action — setting clear cyber security expectations; increasing transparency and disclosure; and protecting consumer rights. To set clear minimum expectations we are considering greater use of cyber security standards for corporate governance, personal information and smart devices. To increase transparency we are considering initiatives on cyber security labelling for smart devices, vulnerability disclosure and health checks for small businesses. In the area of consumer rights we are seeking your views about appropriate legal remedies for victims. We also welcome feedback on any other policies you would like us to explore. You can find a one-page summary of each proposed policy option below.

Cyber security is a shared responsibility between governments, businesses and the community, and we are committed to working with you on the design of any new policy. We strongly encourage you to make a submission on any of the issues covered in this paper. We will consider all submissions and meet with a wide range of stakeholder groups to fully understand the best ways to grow a prosperous and secure digital economy, before advising Government on next steps.

1 Further information is available from https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems.

Quick overview

Our goal

To make Australia's digital economy more resilient to cyber security threats

How will we get there?

Create stronger incentives for Australian businesses to invest in cyber security

Key areas of action

Set clear expectations	Increase transparency and disclosure	Protect consumer rights
There should be clear minimum expectations for businesses to manage cyber security risks.	Businesses and households should have clear information about the security of technology products.	Consumers should have clear legal remedies after a cyber security incident occurs.

Possible new policies

Governance standards for large businesses (Chapter 4)	Labelling for smart devices (Chapter 7)	Clear legal remedies for consumers (Chapter 10)
Minimum standards for personal information (Chapter 5)	Responsible disclosure policies (Chapter 8)	
Standards for smart devices (Chapter 6)	Health checks for small businesses (Chapter 9)	

Governance standards for large businesses

ONE POSSIBLE APPROACH

Voluntary governance standard for large businesses

Co-designed with industry

Principles-based, not prescriptive

Aligned with international standards

WHY TAKE ACTION?

- Consistent feedback to Government
- Variable understanding of cyber security risk by large businesses
- Advice of the Cyber Security Strategy Industry Advisory Panel
- Business leaders are best placed to drive the cyber resilience of their firm

WHO WOULD BE IMPACTED?

Large businesses and company boards

BENEFITS

Improved management of cyber security risk

Flexible approach

Would complement existing obligations

COSTS & LIMITATIONS

Voluntary to implement. Costs will depend on the content of the standard

Level of uptake unknown

Need to avoid 'tick-a-box' compliance culture

SEEKING YOUR VIEWS...

- What is the best approach to strengthening corporate governance of cyber security risk? Why?
- Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Minimum standards for personal information

ONE POSSIBLE APPROACH

Cost-effective, minimum protections for personal information

Targeted, risk-based approach across the economy

Enforceable code under the Privacy Act

Co-designed by industry

WHY TAKE ACTION?

- 39% of breaches of personal information are caused by cyber security incidents
  - Foundational cyber security controls can mitigate a significant number of cyber incidents
- The Industry Advisory Panel recommended faster adoption of cyber security standards

WHO WOULD BE IMPACTED?

Some businesses covered by the Privacy Act depending on scope

BENEFITS

Increased incentives to improve security

Improved clarity about how to meet existing obligations under the Privacy Act

Controls could be targeted, flexible, scalable and achievable

COSTS & LIMITATIONS

Cost would depend on scope

Would only apply to the protection of 'personal information' and entities covered by the Privacy Act

Would need to be updated over time

SEEKING YOUR VIEWS...

- Would a cyber security code under the Privacy Act be effective? Why or why not?
- What technical controls should be included?
- What technologies, sectors or types of data should be included?

Mandatory product standard for smart devices

ONE POSSIBLE APPROACH

No universal default passwords

Vulnerability disclosure policy

Secure software updates

WHY TAKE ACTION?

- Voluntary Code of Practice has limitations
- International leadership from the UK

WHO WOULD BE IMPACTED?

- Manufacturers of smart devices
- Retailers, wholesalers and online marketplaces that sell smart devices

BENEFITS

Consistent and timely improvements to security

Consumers less vulnerable to threats

COSTS & LIMITATIONS

Costs relatively low based on UK estimates

Minimum requirements, rather than best practice

SEEKING YOUR VIEWS...

- What is the best approach to strengthening the cyber security of smart devices in Australia? Why?
- If so, should we adopt internationally recognised standards (ESTI EN 303 645)?
- What would be the costs?
- Would there be unintended consequences on the Australian market?

Labelling for smart devices

POSSIBLE APPROACHES

★★☆☆☆

Voluntary star rating

or

SUPPORTED UNTIL 2022

Mandatory expiry date

WHY TAKE ACTION?

- Consumers do not have access to clear, accessible information about the cyber security of smart devices
- A recommendation of the Industry Advisory Panel

WHO WOULD BE IMPACTED?

- Manufacturers of smart devices
- Retailers, wholesalers and online marketplaces that sell smart devices

BENEFITS

An internationally aligned approach

Could drive market to compete on security

Could complement a mandatory standard

COSTS & LIMITATIONS

Costs relatively low based on UK estimates. Will vary based on testing requirements

Australia would be the first to mandate an expiry date label

Uptake of voluntary label unknown

SEEKING YOUR VIEWS...

- Is a label for smart devices the best approach to encouraging consumers to purchase secure smart devices? If so, should it be voluntary or mandatory?
- Would a combination of labelling and standards be effective?
- Should mobile phones be included?
- Should the label be digital and physical?

Responsible disclosure policies

ONE POSSIBLE APPROACH

Voluntary guidance or tool-kits for industry

Supporting businesses to partner with security researchers

Enhancing transparency and accountability

WHY TAKE ACTION?

- Adoption of responsible disclosure policies among Australian businesses remains low
- Increasing adoption in international markets

WHO WOULD BE IMPACTED?

Software developers and businesses providing services online

BENEFITS

More software vulnerabilities may be identified

Businesses empowered to adopt best practices

Flexible approach that could be shaped by industry preferences

COSTS & LIMITATIONS

Low costs for industry

Uptake unknown

SEEKING YOUR VIEWS...

- Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? Why or why not?

Voluntary health check for small businesses

ONE POSSIBLE APPROACH

Participating small businesses awarded a trust mark following self-assessment of compliance

Aligned with existing guidance provided by the Australian Cyber Security Centre

Based on successful international programs

WHY TAKE ACTION?

- Small businesses have limited time, limited money and limited cyber security expertise
- Government wants to minimise regulation on small businesses

WHO WOULD BENEFIT?

- Small businesses
- Customers of small businesses

BENEFITS

Improved security outcomes for SMEs leading to improved supply chain security

Commercial benefits for participants

Improved cyber security understanding among small businesses

COSTS & LIMITATIONS

Voluntary to participate

Uptake unknown – additional incentives may be required

SEEKING YOUR VIEWS...

- What is the best approach to strengthening supply chain security for small businesses?
- Would small businesses benefit commercially from a voluntary health check?
- What other incentives would be required to encourage uptake?

Clear legal remedies for consumers

REFORMS CURRENTLY BEING CONSIDERED

Australian Consumer Law (ACL)

Review of the *Privacy Act 1998*

- Civil prohibition for consumer guarantees
- Clearer application of ACL to digital products

- Direct right of action for privacy breaches

WHY ARE REFORMS BEING CONSIDERED?

There are limited legal options for consumers to seek remedies or compensation for cyber security incidents

WHO WOULD BE IMPACTED?

Entities covered under the ACL and Privacy Act

BENEFITS

Appropriate compensation for consumers

Greater incentives for businesses to implement strong cyber security

COSTS & LIMITATIONS

Will depend on exact reforms

SEEKING YOUR VIEWS...

- What issues have arisen to demonstrate any gaps in the ACL in terms of its application to digital products and cyber security risk?
- Are the reforms already being considered to the ACL and Privacy Act to protect consumers online sufficient for cyber security?