Australia’s cybersecurity strategy: cash for cyber-police and training but the cyber-devil is in the cyberdetail

Damien Manuel, *Deakin University*

Australia’s long-awaited cybersecurity strategy, released yesterday, pledges to spend A$1.67 billion over the next ten years to improve online protection for businesses, individuals and the country as a whole.

The lion’s share of the cash will go towards policing and intelligence, with smaller amounts set aside for a grab bag of programs from cybersecurity training to digital ID. Much detail remains to be revealed, and whether the strategy succeeds in improving in the safety of all Australians will depend on how well it is executed over the coming decade.

The winners

As already announced on June 30, the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) (which is based within the ASD) are big winners. They will jointly receive A$1.35 billion over the next ten years.

The funding will be used to:

- fight cybercrime
- build a new system to share information with industry about the tactics and operations of hackers, criminal syndicates and hostile foreign governments
- implement technology and processes to block malicious websites and viruses before they reach millions of Australians
- expand data science and intelligence capabilities (in other words, more cyber spies)
- establish new research laboratories
- transform the Joint Cyber Security Centres managed by the ACSC, including the placement of outreach officers to help support small and medium-sized businesses.

These businesses will be able to contact the ACSC for online cyber training to upskill staff and access a round-the-clock helpdesk for advice and assistance. It’s unclear how the government plans to assess this service, but high-quality advice and rapid response will be the keys for success.

The government will also implement an awareness campaign targeting small business, older Australians and Australian families to help improve community cyber safety. This is a long-overdue measure, but it will need to be sustained and to resonate with the target audience to change the security culture and behaviour of Australians.

The losers

The remaining A$320 million, or A$32 million per year over ten years, will be spread over many programs largely aimed at businesses and the education sector.

Large businesses and service providers will be “encouraged” by the federal government to create tools and bundles of secure services to offer to small businesses. The cost of these secure services is unclear.

How the promised “encouragement” will occur is also open to interpretation. It may be the stick

approach, with legislation, or the carrot, via tax incentives or grants.

This strategy has its dangers. The federal government may appear to be picking winners and losers in a complex ecosystem of service providers.

Wait and see

Cyber security professionals will be regulated to ensure clear professional standards, like plumbers and electricians. This is a good thing, but again, the details will be extremely important, such as who performs the accreditation, what framework they use, and how the program is overseen.

Businesses and academia will also receive yet more “encouragement”, this time to partner together to find innovative new ways to improve cyber security skills. This means an injection of A$26.5m into the Cyber Skill Partnership Innovation Fund, as part of the Cyber Security National Workforce Growth Program.

The fund will help support scholarships, apprenticeships, retraining initiatives, internships and other activities that meet the need of businesses. It sounds exciting, but again it is light on details and metrics.

The strategy also discusses using digital identities such as myGovID to “make accessing online services easier and safer”. While this will help prevent identity theft and may be more convenient, it does raise the spectre of the return of the Australia Card concept. This national central identity register was proposed by the Hawke government in 1985.

We can also expect to see additional legislation introduced later this year, forcing critical infrastructure and systems of national significance to improve their cyber security. This is no bad thing, but it is unclear whether consumers or government will end up paying for it.

Execution of the strategy will be key

An Industry Advisory Committee will be established to guide and oversee the implementation of the strategy. Members of this extremely important committee are yet to be announced.

To be effective, the committee needs to include people from a variety of sectors such as healthcare, retail, manufacturing, finance, agriculture and education. As the government’s strategy makes clear, there is no one-size-fits-all solution for cyber security. The members of the committee must reflect a wide range of needs and diversity.

It is too early to tell whether the proposed strategy will deliver the right outcomes for Australian organisations, families and individuals. Until the strategy is executed, we won’t know whether and how it will deliver the promised safety improvements for all Australians.

Damien Manuel, Director, Centre for Cyber Security Research & Innovation (CSRI), *Deakin University*