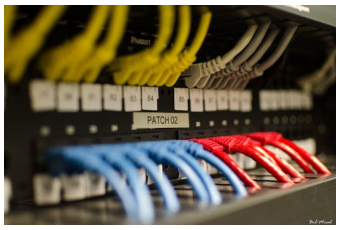

Australia's cybersecurity strategy needs some work. Bob Mical/Flickr , CC BY-NC-SA

Prime Minister Malcolm Turnbull launched Australia's cybersecurity strategy in April 2016, and more than one year on, there's work to be done.

Upon launch, the strategy was criticised for its lack of funding and vague goals. Among other targets, it aimed to ensure more information was shared between government agencies and the private sector about cyber threats, and that universities were training "skilled cyber security professionals".

*The recent Australian Strategic Policy Institute's (ASPI) publication “Australia’s cyber security strategy: execution & evolution”
is something of a report card on the government's progress so far. The aim of the strategy was to improve the security of Australian government organisations as well as businesses and individuals, and while ASPI said there had been "significant encouraging progress", it also noted investment in a number of key goals has been insufficient.*

We asked a panel of experts to weigh in: how is the government doing 12 months into its cybersecurity strategy?

Ritesh Chugh, Senior Lecturer, School of Engineering & Technology, CQUniversity

As the initial 2016 cybersecurity strategy did not specify quantifiable outcomes for most of its five action plan items – (1) national cyber partnership, (2) strong cyber defences, (3) global responsibility and influence, (4) growth and innovation and (5) cyber smart nation – measuring its progress in the ASPI report is difficult.

An absence of adequate implementation plans as well as poor methodology is evident in the government's strategy, as witnessed in the bungled 2016 Census , as ASPI mentions. It appears the strategy has also not been fully implemented due to lack of government spending on cyber issues, and inadequate human resource allocation. However, there are lessons to learn.

Education and public awareness will continue to play a vital role in ensuring people are better prepared for cyber threats. The Stay Smart Online website is a good initiative and can be enhanced by encouraging more people to sign up to its Alert Service . Communication should continue to be a key focus.

For the strategy to work effectively, it is also important that better public-private partnerships are established. Small to medium enterprises (estimated to be around 95% of all businesses) form a large part of the Australian landscape and are relatively easy targets. Awareness and educational programs more specifically tailored to their needs are warranted, along with easy access to experts in cybersecurity – perhaps a phone support contact centre.

It is necessary for the government to consider their commitment to the strategy.

Leonie Simpson, Senior Lecturer, Science and Engineering Faculty, Queensland University of Technology

ASPI recommends the government communicate more openly with the private sector, suggesting quarterly threat reporting be issued from the Australian Cyber Security Centre along with regular strategy updates to give confidence to the community.

In my view, that's an important step. The Australian Computer Crime and Security Survey series published from 2002 to 2006, for example, gave insight into cybersecurity in the Australian context. Its discontinuation, along with the lack of breach notification (until 2017), left a void in public reporting on commonly occurring cyber incidents, which is important in informing cyber

risk management of both public and private organisations.

Although there have been similar reports in years since, a regular series from Australian Cyber Security Centre (ACSC) could be highly useful.

As yet, we have not seen much progress on actions under the “Cyber Smart Nation” theme . Academic Centres of Cyber Security Excellence have not yet been established, although the process is underway.

ASPI’s recommendations also do not target gender bias specifically, although it notes in the report that the government has been “proactively tackling” the issue via its 2016 Australian Cyber Security Challenge, among other initiatives.

Recommendation 9 suggests we broaden the concept of cyber skill shortages to include other disciplines, including law, psychology, communications and so on. This may indirectly assist in increasing cyber workforce diversity, but it does not address the common misconception that women or other minority groups do not hold or wish to hold technical security roles.

This is an area that may benefit from other programs, such as the Science in Australia Gender Equity (SAGE) pilot. The predicted cybersecurity workforce shortages make addressing diversity a priority.

Asif Gill, Senior Lecturer, School of Software, University of Technology Sydney

The ASPI report highlights encouraging progress and commitment from both the government and private sector to Australia’s Cyber Security Strategy . Despite this interest, there are some pressing challenges in this report that warrant further analysis.

The report points to the ad hoc nature of the government's communication and expectation management with industry partners. This calls not only for a clear action plan, but also active stakeholder communication to effectively engage and enact the strategy, and quantitatively track and measure its progress.

The stategy's five interdependent themes could also be more precisely integrated, prioritised and planned in an ordered cybersecurity value chain to streamline efforts and achieve success incrementally.

For instance, core to cybersecurity is to the ability to effectively and proactively defend against cyber attacks. But the report highlighted a recent Australian National Audit Office audit that found two key government departments had "insufficient protection" against external cyber attacks.

Further, the strategy’s ambitious list of 33 initiatives, from appointing a Cyber Ambassador to co-designing voluntary cybersecurity "health checks" for ASX100 listed businesses, seems too many.

It would be better to identify a small and manageable set of high value initiatives and action them, with the ability to refine and edit as new information emerges. Initiatives identified today may become quickly irrelevant due to rapid changes in the cybersecurity landscape in the next three years or so.

Asif Q Gill is a member of DAMA.

Leonie Simpson is a member of the International Association for Cryptologic Research.

Ritesh Chugh does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond the academic appointment above.

Authors: Ritesh Chugh, Senior Lecturer (Information Systems Management), CQUniversity Australia

Read more http://theconversation.com/one-year-on-is-australias-cybersecurity-strategy-on-track-experts-respond-78675