# New guidelines for responding to cyber attacks don't go far enough

December 18 2018, by Adam Henry

Credit: AI-generated image (disclaimer)

Debates about cyber security in Australia over the past few weeks have largely centred around the passing of the government's controversial Assistance and Access bill. But while government access to encrypted messages is an important subject, protecting Australia from threat could depend more on the task of developing a solid and robust cyber security

response plan.

Australia released its first Cyber Incident Management Arrangements (CIMA) for state, territory and federal governments on December 12. It's a commendable move towards a comprehensive national civil defence strategy for cyber space.

Coming at least a decade after the need was first foreshadowed by the government, this is just the initial step on a path that demands much more development. Beyond CIMA, the government needs to better explain to the public the unique threats posed by large scale cyber incidents and, on that basis, engage the private sector and a wider community of experts on addressing those unique threats.

## Australia is poorly prepared

The aim of the new cyber incident arrangements is to reduce the scope, impact and severity of a "national cyber incident".

A national cyber incident is defined as being of potential national importance, but less severe than a "crisis" that would trigger the government's Australian Government Crisis Management Framework (AGCMF).

Australia is currently ill-prepared to respond to a major cyber incident, such as the Wannacry or NotPetya attacks in 2017.

Wannacry severely disrupted the UK's National Health Service, at a cost of A$160 million. NotPetya shut down the world's largest shipping container company, Maersk, for several weeks, costing it A$500 million.

When costs for random cyber attacks are so high, it's vital that all Australian governments have coordinated response plans to high-threat

incidents. The CIMA sets out inter-jurisdictional coordination arrangements, roles and responsibilities, and principles for cooperation.

A higher-level cyber crisis that would trigger the AGCMF (a process that itself looks somewhat under-prepared) is one that "… results in sustained disruption to essential services, severe economic damage, a threat to national security or loss of life."

## More cyber experts and cyber incident exercises

At just seven pages in length, in glossy brochure format, the CIMA does not outline specific operational incident management protocols.

This will be up to state and territory governments to negotiate with the Commonwealth. That means the protocols developed may be subject to competing budget priorities, political appetite, divergent levels of cyber maturity, and, most importantly, staffing requirements.

Australia has a serious crisis in the availability of skilled cyber personnel in general. This is particularly the case in specialist areas required for the management of complex cyber incidents.

Government agencies struggle to compete with major corporations, such as the major banks, for the top-level recruits.

The skills crisis is exacerbated by the lack of high quality education and training programs in Australia for this specialist task. Our universities, for the most part, do not teach – or even research – complex cyber incidents on a scale that could begin to service the national need.

The federal government must move quickly to strengthen and formalise arrangements for collaboration with key non-governmental partners – particularly the business sector, but also researchers and large non-profit

entities.

Critical infrastructure providers, such as electricity companies, should be among the first businesses targeted for collaboration due to the scale of potential fallout if they came under attack.

To help achieve this, CIMA outlines plans to institutionalise, for the first time, regular cyber incident exercises that address nationwide needs.

## Better long-term planning is needed

While these moves are a good start, there are three longer term tasks that need attention.

First, the government needs to construct a consistent, credible and durable public narrative around the purpose of its cyber incident policies, and associated exercise programs.

Former Cyber Security Minister Dan Tehan has spoken of a single cyber storm, former Prime Minister Malcolm Turnbull spoke of a perfect cyber storm (several storms together), and Cyber Coordinator Alastair McGibbon spoke of a cyber catastrophe as the only existential threat Australia faced.

But there is little articulation in the public domain of what these ideas actually mean.

The new cyber incident management arrangements are meant to operate below the level of national cyber crisis. But the country is in dire need of a civil defence strategy for cyber space that addresses both levels of attack. There is no significant mention of cyber threats in the website of the Australian Disaster Resilience Knowledge Hub.

This is a completely new form of civil defence, and it may need a new form of organisation to carry it forward. A new, dedicated arm of a existing agency, such as the State Emergency Services (SES), is another potential solution.

One of us (Greg Austin) proposed in 2016 the creation of a new "cyber civil corps". This would be a disciplined service relying on part-time commitments from the people best trained to respond to national cyber emergencies. A cyber civil corps could also help to define training needs and contribute to national training packages.

The second task falls to private business, who face potentially crippling costs in random cyber attacks.

They will need to build their own body of expertise in cyber simulations and exercise. Contracting out such responsibilities to consulting companies, or one-off reports, would produce scattershot results. Any "lessons learnt" within firms about contingency management could fail to be consolidated and shared with the wider business community.

The third task of all stakeholders is to mobilise an expanding knowledge community led by researchers from academia, government and the private sector.

What exists at the moment is minimalist, and appears hostage to the preferences of a handful of senior officials in Australian Cyber Security Centre (ACSC) and the Department of Home Affairs who may not be in post within several years.

Cyber civil defence is the responsibility of the entire community. Australia needs a national standing committee for cyber security emergency management and resilience that is an equal partnership between government, business, and academic specialists.