

Individuals not the priority in the Cyber Security Strategy

Written by The Conversation USA

The [Cyber Security Strategy announced today](#) by Prime Minister Malcolm Turnbull clearly places a high priority on protecting Australian government systems from foreign powers.

But when it comes to protecting citizens' personal information, it appears to be rather a mixed bag.

While very short on specifics, it does announce several potentially useful initiatives that may help protect Australians against cybercrime. But notably absent is any pressure on the private sector to improve its cybersecurity efforts.

First, it commits the government to increasing the number and training of cybersecurity specialists in the [Australian Federal Police](#) and [Australian Crime Commission](#) .

The government also wants to get its own house in order, in part by conducting additional independent security assessments of internal federal government IT infrastructure.

This is an interesting move given [Turnbull today confirmed](#) both the Bureau of Meteorology and the Department of Parliamentary Services had been the [victim of recent cyberattacks](#) .

But if more externally focused departments, such as the Australian Tax Office, Centrelink and Medicare, are also thoroughly audited, it would reduce the risk of those organisations' large collections of personal data being compromised by criminals.

The strategy talks about sponsoring research to better understand the cost of malicious cyberactivity to the Australian economy. It says figures vary, with some putting the cost of cybercrime in Australia at about A\$1 billion a year, but other estimates put it as high as A\$17 billion.

But perhaps the most useful contributions to cybersecurity for the broader public come from two measures:

-

Increasing the number, and skills, of graduates with cybersecurity expertise in both the university and TAFE sector, and

-

Partner with a range of organisations to “deliver a sustained, national awareness raising campaign, encompassing a range of activities, which enables all Australians to be secure online”.

The effectiveness of both of these policies depends on how they are actually implemented.

In tertiary education, it's easy enough to devote a couple of lectures and an exam question to the topic, to tick an auditing body's box marked “cybersecurity”.

Making sure that our students actually know how to design, build and operate secure systems is a much tougher challenge. It's one that my colleagues and I at Monash University, and our counterparts at universities around Australia, are working hard on.

Is it enough?

The biggest cybersecurity threat to individuals remains the unauthorised use of their personal information to commit a variety of financial crimes. It is here that the Cyber Security Strategy seems to lack focus.

Prevention is usually better than cure, and in the case of cybercrime committed across national boundaries, law enforcement is often ineffective. It will likely remain so, despite the worthy rhetoric in the strategy about international cooperation.

Therefore, the primary defence we have is making sure the organisations that hold our personal data are taking sufficient measures to prevent cybercriminals from gaining access. Many of these organisations are in the private sector.

But the government is relying on hints and a bit of assistance to get the private sector to improve its efforts in this area. This is perhaps unsurprising, given the antipathy to “red tape” of the current government.

For example, when the strategy mentions raising the bar, it says:

Self-regulation and a national set of simple, voluntary guidelines co-designed with the private sector will help organisations improve their cyber security resilience.

One might have thought our largest businesses would already have the financial means to hire external consultants to assess their security strategies. But ASX 100 listed businesses are to be offered voluntary “health checks”:

The governance ‘health checks’ will enable boards and senior management to better understand their cyber security status and how they compare to similar organisations.

As for small business, the strategy acknowledges they might not allocate enough resources to cybersecurity and they could become a “soft underbelly or back door into connected organisations”.

To deal with that, the government plans to offer tests of what cybersecurity measures small businesses have in place by certified practitioners.

Flogging business with a wet lettuce leaf

But there's no shortage of information security guidelines available to organisations already. In far too many cases, what is lacking is the will to implement them.

Unfortunately, in practice, the consequences for security breaches seem extraordinarily limited. The breaches of the Privacy Act to date result in financial penalties that are trivial for large organisations.

For instance, [Telstra was fined](#) a grand total of A\$11,000 for a breach involving thousands of customers.

Further, companies aren't even obligated to inform their customers of a breach, unlike in the United States and European Union.

While all this has gone unmentioned in the strategy, the government has been working on a "mandatory data breach" notification law for some time. But it seems in no hurry to actually make it law.

A [draft bill](#) was released for comment in late 2015. As of today it still hasn't been introduced into parliament, and the draft exempts organisations with annual turnover of less than A\$3 million.

Cybersecurity breaches in private sector companies sometimes do have negative consequences for those companies. But they also inflict significant and often larger consequences on the people whose personal data is stolen.

And it's the role of governments to step in with some kind of regulation when an action creates significant negative impacts on citizens.

But the current government seems to have decided that the costs to business of forcing them to take cybersecurity seriously outweigh the benefits.

Individuals not the priority in the Cyber Security Strategy

Written by The Conversation USA

~~Report that is obtained from this website has disclosed by any~~