Cyber strategy needs user centric design

James Riley Editorial Director 18 August 2020

The federal government's $1.7 billion 2020 Cyber Security Strategy document lacked the kind of strong organising principle to adequately address the cyber challenges of the less secure world, according to ANU Cyber Institute chief executive Lesley Seebeck.

The strategy will need a significant structural re-working if Australia is to meet the challenge of a post-COVID world described by the Prime Minister Scott Morrison as "poorer, more dangerous and more disorderly."

Home Affairs had produced a cybersecurity document that was admirably broad – from the personal cyber issues to creating economic advantage through cyber to national security cyber issues.

But it did not reflect the multi-dimensional complexities of cyber issues and all of inter-related and overlapping parts of the economic and social systems that must be secured.

In this podcast interview with *InnovationAus*' Commercial Disco, Prof Seebeck argues the case for a "user-centered design version" of the document – one that will grab the attention and earn the attention of citizens and businesses.

Prof Seebeck, who is a professor in the practice of cybersecurity – and also a member of the government's Naval Shipbuilding Advisory Board – says despite the breadth of discussion, the document does not reflect just how embedded information systems are across the economy, government and the individual lives of its citizens.

This is not well understood by "the citizens on the street, and I don't think its really been grasped by the various different levels of government."

"Because there is not an organising principle in that document and because there is no vision of the future except that 'it's getting bad' – and we already knew that – this document really struggles," Prof Seebeck said.

"We are relying more and more on the internet [and] the pressure is growing. The Prime Minister has already flagged the fact that we are heading for a darker, poorer world, and so those [cyber] resources are likely to be less available," she said.

Cybersecurity "is going to be harder, and frankly I do not believe this document is going to … ensure protection. You need to have an organising principle."

"Home Affairs has gone for breadth. They have tried to cover off everything. But because cyber cybersecurity is so multidimensional, there isn't a prioritization mechanism. Once you have got the big picture of what you want the future to look like for the country – the organising principle – then you are able to set priorities and allocate resources," Prof Seebeck said.

"And that will give you a coherent strategy, which you can then roll out," she said. "It's fully understandable that they were trying to cover off as many things as they did, but it's a bit of a grab-bag as a result.

“What you need there is a conceptual structure that gives it some shape and form. That’s what’s missing.”

The cybersecurity strategy includes deep and difficult policy issues that need to be tackled – everything from sovereignty to industry policy to skills development and building out an ecosystem, and targeted R&D .

And there was enormous work to be done in understanding the international environment and formulating ways to work together with “fellow democracies” to stabilise and secure the internet.

“There is a lot of policy work and strategy work that needs to get done. Now that’s not going to be done just by doing some community consultations,” Prof Seebeck said.

“This is hard work. This is where you need serious intellectual grunt.”