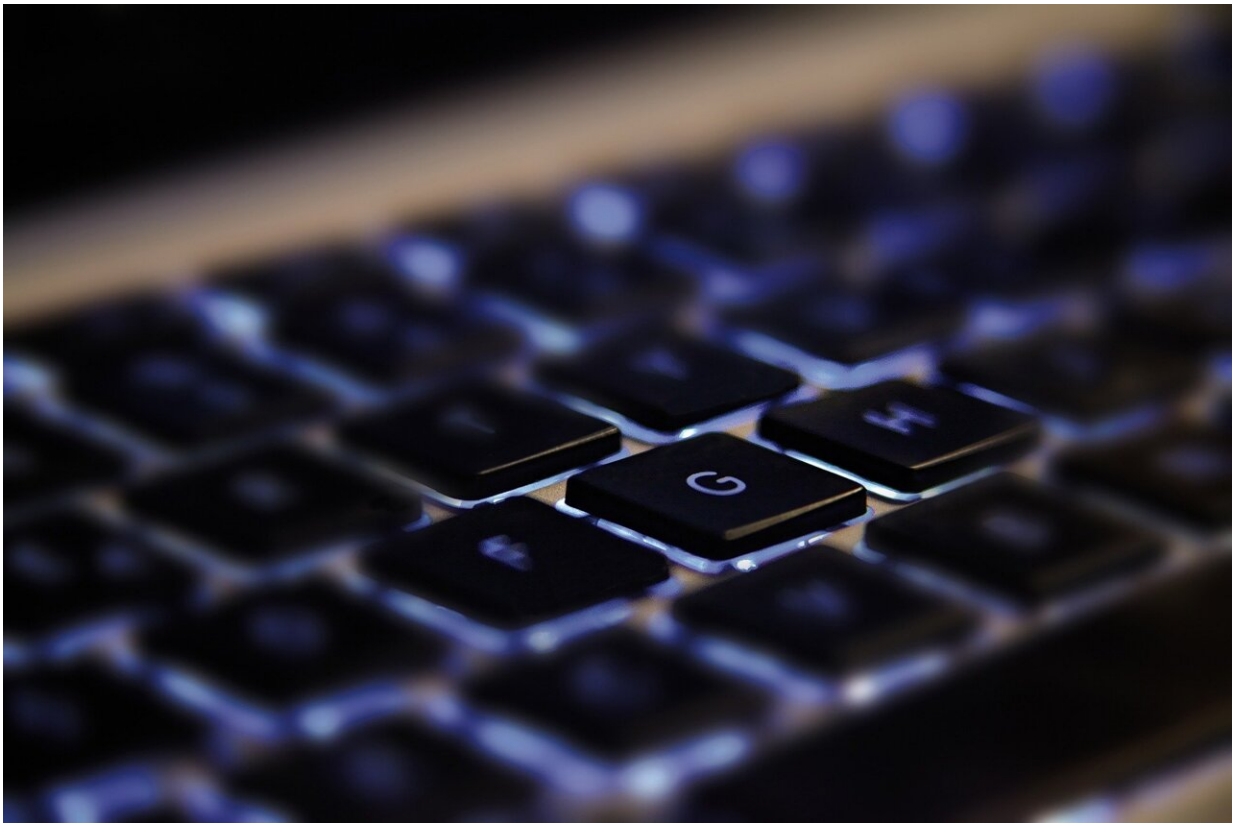
Australian public wants to build cyber resilience, say researchers

November 16 2022



Credit: Pixabay/CC0 Public Domain

Illegal cyber attacks on thousands of citizens' personal data in Australia has heightened awareness of the hazards of insecure digital systems—and Flinders University researchers say consumers want to

play a more active role in building more resilient systems to reduce risks caused by hacking, online deception, bots and other threats.

Their study of a nationally representative sample of 1,500 Australian citizens in 2020—and focus groups comprising 62 people in three states—investigated attitudes to institutional trust, understanding of resilience, digital literacy and perceptions of cyber threats.

Even before the escalation in recent cyber breaches of Optus and Medibank Private customer bases, citizens in the surveys were clearly not confident or optimistic that Australia is keeping pace with cyber threats and interference in the country's economy, politics or society.

"Not only are these citizens concerned about the technological capabilities of government—often citing poor experiences using online government services—but they also showed doubts about investment in skills and commitments to cybersecurity among businesses," says Flinders University researcher Dr. Josh Holloway.

"Quite reasonably, they tended to have little awareness of which public institutions and authorities are taking leadership in managing cyber threats and, collectively, expressed broad skepticism of social media and tech companies, media organizations, the federal government and public service generally."

While survey participants wanted more capability and responsibility from the public sector and corporations, their trust in this process was low.

The findings, published in the journal *Defence Studies*, highlights the gap between Australian citizens' knowledge and engagement and the broad response to cyber threats from top-down, technocratic and elite-driven agencies.

Co-author Associate Professor Robert Manwaring says Australian citizens' confusion and lack of trust is not necessarily their fault.

"There's generally little meaningful strategic effort to engage citizens in government-led responses, overlooking what's often called the 'social layer' of cybersecurity," says Associate Professor Manwaring.

"We need to encourage a genuinely whole-of-society approach—something which like Sweden and Finland are making considerable inroads."

The media also should play a greater role in informing the public and public debate around cyber threats.

"There's clear scope for more nuanced, regular coverage of cyber risks—and one that is less focused on international 'spectacle' and reactive coverage.

"Australians need to be informed of the reality of cyber risk, and given the tools and information to participate in strategic efforts to enhance Australia's cyber resilience, rather than just hearing about the fallout of successful cyber-attacks."

The article, "Resilience to cyber-enabled foreign interference: citizen understanding and threat perceptions," is published in *Defence Studies*.

More information: Rob Manwaring et al, Resilience to cyber-enabled foreign interference: citizen understanding and threat perceptions, *Defence Studies* (2022). DOI: 10.1080/14702436.2022.2138349

Provided by Flinders University