

# Disinformation campaigns biggest potential threat to future Australian elections

With all eyes on the upcoming US Presidential election, ANZ IT professionals weigh in on the future of election security.

Sydney, Australia (16 September 2020) – IT professionals across Australia and New Zealand (ANZ) believe disinformation campaigns are the biggest potential threat to elections in our region, according to new research survey released today by nonpartisan, global technology association ISACA. Misinformation campaigns ranked at 72% amongst respondents, who also identified hacking or tampering with voter registration rolls (49%) and tampering with the tabulation of voter results (44%) as the other potential top threats to election security. More than half (57%) believe at least one of these threats will significantly impact the outcome of future national elections.

“Given the recent headlines about nation-state cyber attacks in Australia, and news about misinformation campaigns through social media in the upcoming US presidential election, it’s not surprising that IT professionals view this as a potential threat on our shores,” states Ian Brightwell, CGEIT, Principal Consultant, DH4 and ISACA member.

ISACA surveyed more than 8,500 IT governance, risk, security and audit professionals around the globe regarding election security. Despite possible threats, respondents from ANZ are generally more confident in election security across the board than their counterparts in the United States. 83% are confident in the resiliency of the infrastructure in the national elections, compared to only 63% of respondents in the US. 85% are confident fraudulent votes will not be cast in future elections, compared to 60% in the US. 83% of respondents are confident that their country’s election systems are secure from hacking and other technological threats, compared to 71% in the US.

“The objective of electoral officials is to help facilitate the smooth transition of power. In Australia, there is a high degree of confidence and trust in the electoral process, but these figures indicate the trust in the US has been eroded,” adds Brightwell. “This doesn’t mean that the electoral processes in the US aren’t robust, but that the US officials need to educate constituents on the process to curb disinformation and ensure it doesn’t affect the outcome. Every electoral commission needs to be transparent and have robust processes, standards and testing in place.”

“Proper scrutiny using appropriate external audit controls is critical to maintain the validity of any election process. The outcome of these audits must be communicated in a transparent way to ward off disinformation from internal or external sources about the election’s integrity.”

Interestingly, while just under half (49%) of ANZ respondents believe there is appropriate funding in place to prevent non-technological threats (i.e. human interference or unauthorised polling place access), only 28% believe adequate funding exists to prevent hacking. This signals that either more funding may need to be budgeted for this in future elections or that participants are unaware of the current levels of funding in place to secure elections.

“Adequate funding for voting is essential to maintain the integrity and transparency of the election process. Post-COVID, more funding may be required for national elections from a health and safety perspective. These could include a wider range of voting services and options, such as longer opening times for early voting and postal voting, just as is being implemented for the up-coming Queensland state election in October.

“Australia has conducted electronic voting at a state level in NSW to complement postal voting. This option should be a consideration by all jurisdictions in Australia as long as rigorous external controls are in place to ensure integrity and effective transparency is provided. One advantage of electronic voting would be to enable quicker results than current timeframes for counting of paper ballots,” concludes Brightwell.

The survey found that respondents believe education about misinformation, laws addressing election security and increased training for election security personnel are all key components to ensure voter confidence and accountability.

“As a learning organisation, ISACA has long recognised the power of education. In the case of election security, education has the power to instil confidence, ensure election professionals and volunteers are well trained, and help electorates identify and share information that is accurate instead of information that is intended to manipulate voters’ perceptions,” said Nader Qaimari, ISACA chief learning officer.

###

## About ISACA

For more than 50 years, ISACA® ([www.isaca.org](http://www.isaca.org)) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organisations and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organisation that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including 223 chapters worldwide.

Twitter: [www.twitter.com/ISACANews](https://www.twitter.com/ISACANews)

LinkedIn: [www.linkedin.com/company/isaca](https://www.linkedin.com/company/isaca)

Facebook: [www.facebook.com/ISACAGlobal](https://www.facebook.com/ISACAGlobal)

Instagram: [www.instagram.com/isacanews](https://www.instagram.com/isacanews)

### Contact:

Julie Fenwick, [jfenwick@daylightagency.com.au](mailto:jfenwick@daylightagency.com.au), +61 468 901 655

Karen Keech, [kkeech@daylightagency.com.au](mailto:kkeech@daylightagency.com.au), +61 411 052 408

### **Contacts**

Julie Fenwick  
The Daylight Agency  
mailto:  
Karen Keech  
0411 052 408  
mailto: