Cybersecurity
A PRIORITY ON *VOTING DAY*

iVote® Transforms the Electoral System in New South Wales, Australia

by Jenny Mangelsdorf

The future of voting may already be here. In Australia, an electronic voting system that allows constituents to cast ballots via the Internet and telephone had a successful trial run in a 2011 parliamentary election in the state of New South Wales (NSW).

Originally developed to allow the visually impaired to easily participate in the democratic process, iVote also serves voters with literacy issues, disabilities, those who live more than 20 kilometers from a polling place, or those who are voting from another state or country.

With its initial success, officials are now preparing iVote for its first full operation at the NSW state election in 2015. Because more people are now aware of the iVote option, officials anticipate that many more electors will vote remotely using the system. While iVote isn't intended to replace personal voting and paper ballots, Australia's NSW Electoral Commission (NSWEC) expects a gradual and ongoing increase in user numbers as voters accept the system and as its security and effectiveness are proven.

With many jurisdictions thinking of adopting some form of electronic voting, there is a lot of interest in New South Wales' experience.

Because the technology is still relatively new, the NSW Electoral Commission wanted to ensure that iVote would have the voters' trust. The commission built in user feedback routines that confirm the user's vote is cast as he or she intended, and it adopted an open approach to election-result reporting that lets interested parties check the results in parallel with the commission's results. The commission then looked to CSC to assess what cybersecurity risks might threaten its iVote system.

"When you bring electronic voting into the mix, you have to ensure that the community will trust the outcome," says Ian Brightwell, NSWEC CIO. "Cybersecurity is not our business. Although it's important for an electronic voting system, it's not something we as an organization would have to deal with at the level that CSC deals with on a daily basis. CSC provided us with a view of the cybersecurity landscape, and of initiatives and opportunities we can engage with to improve our security posture."

More voters casting ballots

For NSW's 2015 election, the commission expects that the number of voters taking advantage of iVote will quadruple to more than 200,000, with most being outside the state and most using the Internet to submit their ballots. Because of the increased number of voters saying they plan to use the electronic system, the NSWEC asked CSC to analyze and report what it might encounter with regard to threats to the voting system.

"The iVote initiative is probably the most significant change that we've seen in the electoral processes in the last 100 years," says Colin Barry, NSWEC electoral commissioner. "We wanted to get a better understanding [about] the security of iVote, especially because more people will be using it and its greater prominence on the international stage. When you open those doors, there's always risk."

For the analysis, CSC looked at risks such as impersonation, tampering, ballot-box stuffing, and challenges to integrity and ballot secrecy. CSC also analyzed what types of threats might affect the system and the environment in which the system operates.

"The threats themselves are very dynamic," says Clinton Firth, CSC cybersecurity general manager, Australia and New Zealand. "Threat actors evolve through new affiliations, skills and capabilities, and they target and calibrate their actions. If they're motivated to attack a target, they will continue to attack it even if they hit a roadblock."

Securing transparency and trust

CSC's strategic threat assessment also included war gaming and tabletop exercises to generate additional analyses that would help NSWEC further secure its system. By understanding the types of threat actors that might attack the iVote system, and the landscape in which they operate, CSC helped the NSWEC provide the secrecy, transparency and trust that voters and candidates expect.

"This type of advanced threat-based approach, which focuses on what is happening in the world, is a much better way to secure a system than relying completely on a compliance-based threat approach, which focuses on standards or regulations," Firth says.

"CSC's report opened my eyes to a raft of issues I was not aware of, ranging from people who might be computer hackers sitting at home, to looking at international organizations that have a history of cyberattacking, and even to countries that might have an interest in trying to undermine the integrity of our voting system," says Barry. "This showed the enormity of the potential threats we needed to manage."

Risk always exists, whether using traditional paper-based ballots or electronic ballots such as those generated by NSWEC's iVote system. "The question is, 'Is this a risk that is manageable?'" says Barry. "In my view, I'm confident that the analysis that has been undertaken will allow us to manage those risks and let us move forward with electronic voting in NSW." ■

JENNY MANGELSDORF is a writer for CSC's digital marketing team.

Client: Australia's New South Wales Electoral Commission

Challenge:

- Protect and secure electronic voting system
- Prepare the system for a substantial 2015 voter turnout

Solution:

- Conduct risk analysis of current and potential threats
- Identify possible attackers of voting system
- Analyze iVote vulnerabilities

Results:

- Enhanced cybersecurity awareness
- Decreased risk to iVote system
- Increased government and community trust

Learn more at csc.com/cybersecurity.