

AI SECURITY · AUSTRALIAN BUSINESS · 2026

Talk to Us About How AI Improves Your Security

Australian businesses now report a cybercrime roughly every six minutes, and the average incident costs \$80,850. A large part of what makes the current wave work is that AI made convincing fraud cheap to produce at volume.

The published cost position: more than 84,700 cybercrime reports a year in Australia, about one every six minutes; over 1,200 incidents responded to, up 11%; average cost per incident up 50% to **\$80,850**. \$56,600 for small business, \$97,000 for medium, and \$202,700 for organisations over 200 staff. **AI made the attack side cheap:** convincing phishing at volume, cloned voices, cloned sites. **The same asymmetry runs both ways, and the phone layer is where it pays most,** because voice is where authorisation is given and it is the least monitored channel in most businesses.

■ The short version

Organisation size	Average cost per incident	Change
Small business	\$56,600	Up 14%
Medium business	\$97,000	Up 55%
Large organisations (200+ staff)	\$202,700	Up 219%

Also worth knowing

What AI adds	How it helps
Consistent challenge sequences	The same verification steps every time, in the same order, regardless of how busy, tired or sympathetic the person answering is. Social engineering works on inconsistency.
Cross-checking against the record	What the caller says, checked against what the system holds, while the call is still happening rather than afterwards.
Flagging mismatches for a human	Not refusing service, escalating. The AI notices the discrepancy and hands it to a person with the discrepancy already stated.
Removing the pressure variable	An automated first stage does not feel embarrassed about asking a third question, does not respond to urgency and cannot be flattered.

The important limit, stated up front

This is not voice biometrics and we are not proposing that a voice should be an identity proof. **The whole premise of the current threat is that a voice can be synthesised.** What AI adds here is process consistency and cross-checking, not a magic identification of the human speaking. Any vendor selling you voice-as-password in 2026 is selling you the exact thing that just stopped working.

Questions the full guide answers

- ☐ How much does a cyber incident actually cost an Australian business?
- ☐ Where does AI genuinely improve security on a business phone system?
- ☐ Can AI detect a deepfake or cloned voice on a phone call?
- ☐ What is toll fraud and how does AI help stop it?
- ☐ What can AI not protect my business from?
- ☐ What governance do I need before switching on AI in my phone system?
- ☐ What is the 10 December 2026 automated decision-making obligation?

This is the summary. The guide has the detail.

Every point above is worked through in full on our site, with the Australian context, the numbers and the exceptions. If you would rather talk it through, call **1300 881 662** or visit **unidenvoice.com/get-started**.