SECURITY · INCIDENT ANALYSIS 2026

The RingCentral Breach: What to Do Now

About 1.6 million records of names, emails, phone numbers and addresses. The breach is contained. The phone calls that use that data are just starting.

Sort every statement into one of three columns

Confirmed	Claimed by attackers	Not disclosed
Social engineering attack, July 2026. Disclosed 28 July.	623GB taken in total.	The specific entry technique.
1.6M unique emails with names, phone numbers and addresses, verified by Have I Been Pwned on 13 August.	280GB archive published after RingCentral refused to pay.	Which system held the data, and the forensic findings.
Core platform not affected, services ran normally.	Anything about the unpublished portion.	How many records relate to Australian businesses.

Why contact details are not nothing

A generic call claiming to be your phone company usually fails because it is a guess. A call that names you, quotes your address and refers to a real incident you have read about is a different proposition. **The most valuable field in this leak is the one nobody lists: the fact that you are a customer of this provider.** It tells an attacker exactly who to impersonate.

Five attacks a leaked customer list enables

- **Provider impersonation.** "We are calling about the incident, we need to reset your admin access."
- **Help desk pretext.** Your staff walked onto a fake login page to "re-enrol" their authenticator.
- **Invoice change.** "Following the incident, our bank details have changed."
- **Port-out or SIM swap.** The victim asked to read out the verification code "to confirm identity".
- **Quiet enrichment.** The list merged into bigger datasets and used well into 2027.

The campaign behind it

In 2025 the group behind this phoned staff as IT support and talked them into authorising a fake Salesforce export tool. **Qantas lost data on about 5.7 million customers that way.** From late 2025 it moved to relaying single sign-on logins through fake pages while on the phone, with more than a hundred organisations targeted by January 2026. None of it needed a software flaw. It needed someone to believe a caller.

Do these five this week. They stop real losses

- [ ] **Write down a callback rule.** Access, payment and phone changes are verified on a number you already hold.
- [ ] **Passkeys or hardware keys** on every admin account for phone, email, banking and domain.
- [ ] **Port-out and SIM change lock** on business mobiles that receive codes.
- [ ] **Phone to confirm** any supplier bank detail change before paying.
- [ ] **Brief staff with the actual script**, not a generic phishing warning.

Then tidy the phone system

- Remove admin accounts nobody needs.
- Check call forwarding on main numbers.
- Turn on login alerts and audit logs.
- Bar international and premium numbers.
- Stop users approving new apps alone.

Ask any phone provider

- Where is my contact data held, and by whom?
- How do support staff verify me?
- How will you contact me in an incident?
- Can I require passkeys for admins?
- How are port-out requests authorised?

If you use RingCentral or Optus Loop

Check exposure by typing haveibeenpwned.com yourself, never from a link. Treat any contact about the incident as untrusted until you ring back on a number you already had. Nothing published says Optus Loop customers were affected, but **a business mid-migration is already expecting emails about new logins, which is exactly when a fake one is hardest to spot.**

The breach may be yours to notify as well

Under the Notifiable Data Breaches scheme, a covered business whose personal information is involved in an eligible breach must notify affected people and the OAIC, and must assess a suspected breach within **30 days**. A supplier's notice does not automatically discharge your obligation. Confirm who is notifying, and keep a short record of what you checked and when.