SECURITY LESSONS · 2026

Two Ways In, Both Avoidable

Cisco 2022 came in through a person. Webex 2024 came in through a link. Here is what happened and the fixes a small Australian business can make this week.

The two incidents

	Cisco, 2022	Webex, 2024
Way in	A person, via calls and MFA prompts	A product, via guessable meeting links
Skill needed	Persistence and a calm phone manner	Counting
Key dates	Detected 24 May, disclosed 10 Aug 2022	Reported early May, fixed by 28 May 2024
Exposed	VPN access. ~2.8GB of files later published	Details of 6,000+ government meetings
Who could stop it	The business	Mostly the vendor

The person route, three ordinary decisions

1. **A work password saved in a browser synced to a personal account.** Fix: a business password manager and no personal sync.
2. **Trusting a call from "support".** Fix: one rule, said often. We never ring you to approve a sign-in or read out a code.
3. **One tap on approve.** Fix: number matching for everyone, passkeys for admin, finance and phone system accounts.

Would it have stopped the Cisco route?

Method	Answer
Approve or deny push	**No.** This is what was beaten
SMS or app code	Not reliably. A caller just asks for it
Number matching	Very likely
Passkey or security key	**Yes**

Also switch on

A limit on repeated prompts, and an **alert whenever a new MFA device is added.** The Cisco attacker enrolled their own devices once inside, so they no longer needed the employee at all.

The thirty minute audit

- [ ] Plain approve or deny push is switched off
- [ ] Admin, finance and phone system accounts use passkeys or keys
- [ ] Adding an MFA method alerts somebody
- [ ] Repeated denied prompts are limited
- [ ] Work passwords are not in personal browser profiles
- [ ] Staff have heard "we never ring you for codes"
- [ ] Meetings default to passcode and lobby
- [ ] Calendars show outsiders free or busy only
- [ ] Public recording and file links expire
- [ ] You know who to ring at your provider in an incident

Help desk script

1. No reset on an inbound call alone.
2. Call back on the number on file.
3. Second approval for admin and finance.
4. Notify the owner on another channel.
5. Same rule for everyone, including the boss.

Meeting standard

- New meeting for sensitive topics.
- Passcode, lobby, lock once joined.
- PIN for dial-in.
- Plain titles. Details in the agenda.
- Record with a reason, then delete.

Seven questions for your provider

Ask	Want to hear
How do your staff sign in to my data?	Phishing-resistant MFA
What if someone rings support as me?	Verify, call back, notify
How are meeting and recording links made?	Random, checked, expiring
Would you notice mass link guessing?	Rate limits and alerts
Can I see an access log?	Yes, exportable
Who else touches my calls?	A short named list
How fast would you tell me?	A named process and timeframe

Australian rules

Essential Eight includes MFA and favours phishing-resistant methods for important accounts. Businesses covered by the Privacy Act must assess a suspected breach within 30 days and notify the OAIC and affected people where serious harm is likely.