GOVERNANCE INCIDENT BRIEFING

Briefing | Operations & Governance

EVERY FACE ON THE CALL WAS REAL. THE MONEY WASN'T COMING BACK.

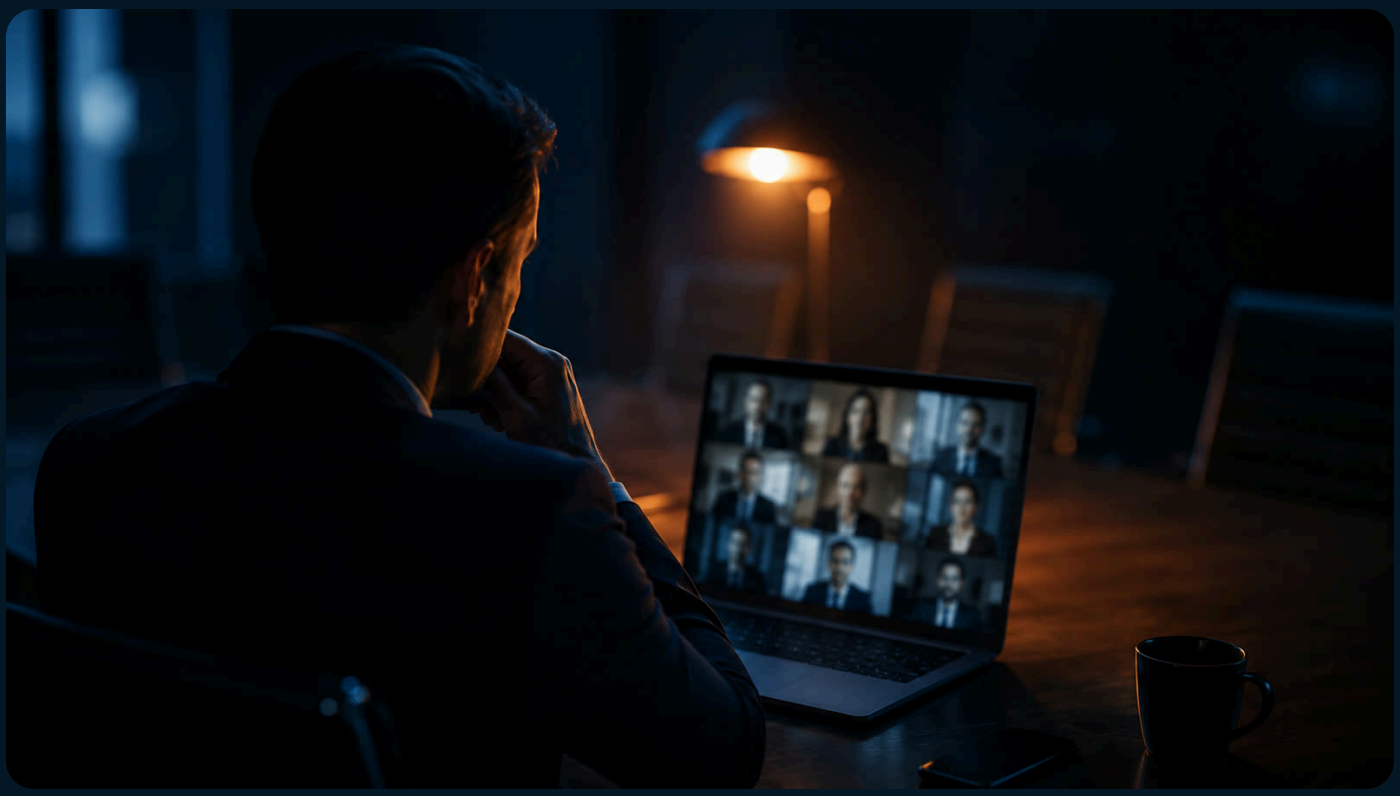
THE $25 MILLION DEEPFAKE THAT BEAT AN EMPLOYEE WHO DID EVERYTHING RIGHT

In January 2024, a finance employee at Arup's Hong Kong office received an email from the company's UK-based CFO requesting a confidential transaction. He was suspicious, phishing emails often look exactly like this, so instead of acting on it, he asked for a video call to confirm.

The call happened. The CFO was there. So were several colleagues he recognised. They looked right. They sounded right. They addressed him by name and confirmed the instructions from the email. His doubts disappeared, and he made fifteen transfers, totalling $25 million, to five Hong Kong bank accounts.

Every single person on that call was a deepfake, built from publicly available footage: recorded meetings, online conferences, the ordinary video content any executive at a company with 18,500 employees generates just by doing their job. Arup's own systems were never breached. No credentials were stolen. Nothing was hacked. As the company's CIO later put it, this wasn't a cyberattack. It was social engineering, just with a far more convincing costume than a well-written email.

The fraud was only discovered when the employee later contacted Arup's actual headquarters to follow up. No such meeting had taken place. No such transaction had been authorised. By then, the money was gone, and as of the most recent reporting, it still hasn't been recovered.



THE GOLD STANDARD OF VERIFICATION, DEFEATED

The verification is what failed him

Most fraud-awareness training still centres on suspicious emails and phone calls: is the sender legitimate, does the request feel rushed, is someone asking you to bypass normal process. The employee did exactly what that training teaches. He was suspicious. He didn't act on the email alone. He asked for verification.

A video call with familiar faces has always been treated as the gold standard of confirmation, the thing you escalate to when an email feels off. That assumption is no longer safe, and most businesses haven't updated their process to reflect it. Arup's own CIO later admitted that, out of curiosity, he tried deepfaking himself using free, publicly available tools. It took him about 45 minutes.

A familiar face on a screen is no longer proof of identity.

The guardrail scales down cleanly

Arup has 18,500 employees and a dedicated finance function. Most businesses don't. But the fix isn't a bigger finance team. A bookkeeper or office manager getting an urgent, confidential payment request from someone claiming to be the business owner, a supplier, or an accountant needs the same rule: no one moves money on a single conversation, however convincing it looked or sounded, and every request gets verified through a channel the request itself didn't supply.

(01) **Independent-channel confirmation**
Payments above a defined threshold require confirmation through a separately verified channel: a callback to a known number, not one supplied on the call.

(02) **No single-person authorisation**
No single employee can authorise a large transfer alone, however convincing the request looked or sounded.

(03) **Deepfake-specific training**
Staff are trained on deepfakes, not just phishing emails, since a familiar face on a screen is no longer proof of identity.

WHERE THIS FITS

This is the sharper edge of a question every business now has to answer: not just which AI tools you use, but what happens when AI is used against you. Propel Growth's Solus Requirements Assessment maps exactly this kind of exposure, where a business's approval processes and financial controls would hold up against a threat that didn't exist three years ago, and where they'd quietly fail.

BOOK A CONFIDENTIAL CONSULTATION

Find out where your own approval processes would actually hold. No obligation, no sales pitch, just a clear read.

↗ **Book a call** ↗

propelgrowth.com.au · +61 452 177 673 (04521 PROPEL) ·
enquiries@propelgrowth.com.au
Level 1, 89 Pirie Street Adelaide, SA 5000 Australia

CNN Business, "Arup revealed as victim of $25 million deepfake scam involving Hong Kong employee" (16 May 2024); AI Incident Database, Incident 634; Adaptive Security, "Arup Deepfake Scam: How $25M Was Stolen via Video Call."