

CISO NEW YORK

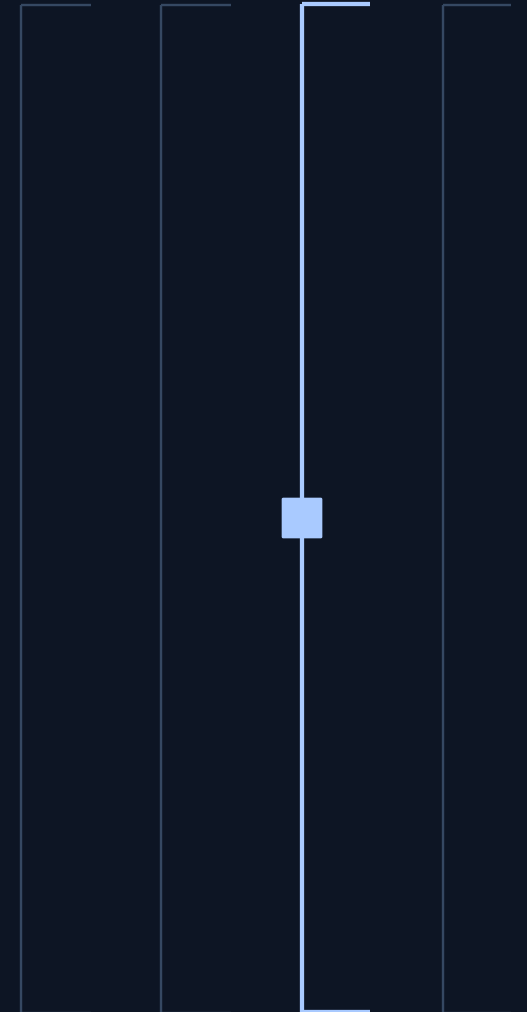
Trust Under Attack

Leading Through the Age
of AI Deception

Liron Golan

Group CISO

Laser Digital · Nomura Group



May 2026, Singapore.

A message. An official-looking
guarantee. An NDA.

A fabricated video meeting
with apparent senior officials.

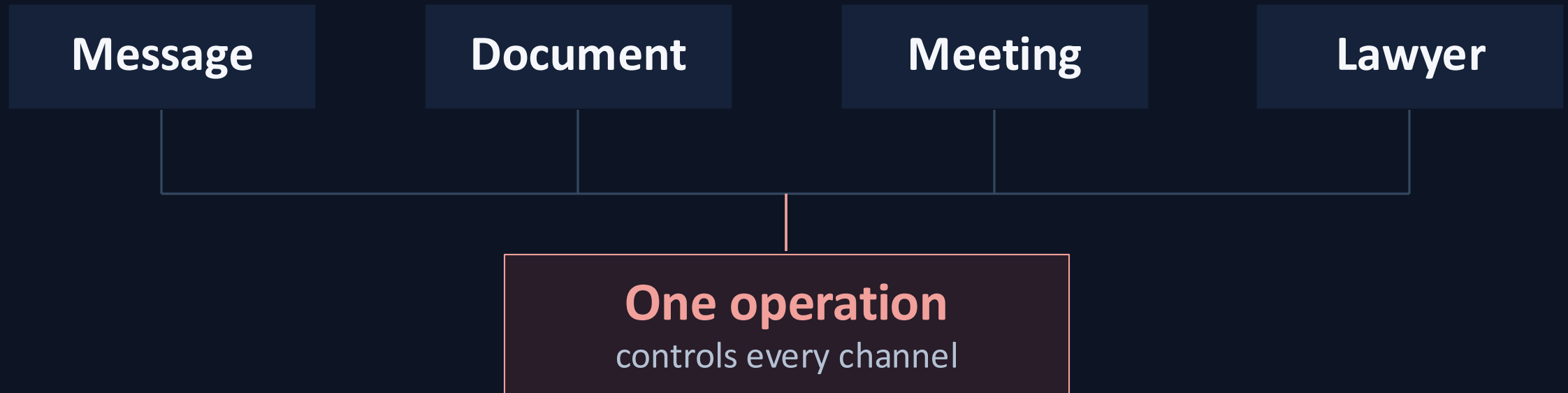
At least SGD

4.9

million transferred.

Source: Singapore Police Force, 14 and 16 May 2026

Several apparent confirmations.
One attacker-controlled operation.



Different formats are not independent evidence.

When the fake is perfect, **what still stops the action?**

A resilience test, not a prediction.

Authenticity is evidence. It is not authorization.

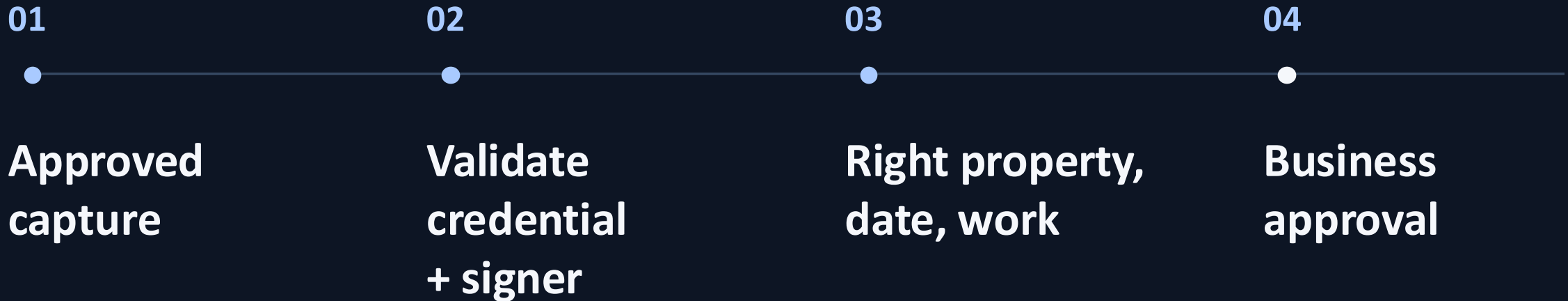
CONTENT CREDENTIALS (C2PA)

What can we establish
about the media?

BUSINESS APPROVAL

What may we do
because of it?

The photo supports the decision.
It does not authorize the payment.



Illustrative: a proposed pattern, not a named lender's deployment.

Verify independently

Verify through a route independent of the request.

Route supplied by the request

The callback number in the email.
The second face on the same call.

Cannot verify? Hold, or approved alternative.

Unreachable is not approval.

Route your organization maintains

Protected contact records.
Verify the specific instruction.

Authorize precisely

Verify the employee

Registered security key
or passkey

If unavailable, use approved
identity verification.

Approve the specific reset

Account

Action

Approved method

Time limit

If the request changes, verify and approve again.

Reward the pause

An urgent request to skip the checks.
Would your employee feel able to pause?

This time, it really is your CFO.

“The board call starts in two minutes. Can you just reset it?”

**The test: may people challenge a real executive,
not just a fake one?**

Decide the response before you need it

**Hold
pending**

**Contact
the bank**

**Contain
access**

**Preserve
evidence**

Communicate

**What if the fake instruction goes to your customers,
not your finance team?**

Business owner for each workflow. Executive sponsor for the program.
The CISO coordinates.

Four questions for the board

01 Which decisions could cause material harm?

02 What stops execution, and when was it tested?

03 Can people pause, even for executives?

04 Who owns the workflow, stopping, and recovery?

A name, not a committee.

Few workflows, ranked by your exposure

Prioritize

High-consequence
workflows

→

Strengthen

Verification + authorization.
Safeguards from day one.

→

Exercise

Under pressure, including
one real request

MEASURE

Verification
before execution

Exceptions

Containment

Added delay

Monday: one workflow, its owner, a convincing impersonation.
Show what stops the action.

01 **Verify independently.**

02 **Authorize precisely.**

03 **Reward the pause.**

Liron Golan · Group CISO, Laser Digital (Nomura Group)