Santander International

10 October 2024

Incident Response

Aviation does it brilliantly, so let’s emulate them in cyber and IT

Dave Cartwright

CISO and Head of Technology Operations & Risk

bcs Fellow

CIISF CHANNEL ISLANDS INFORMATION SECURITY FORUM

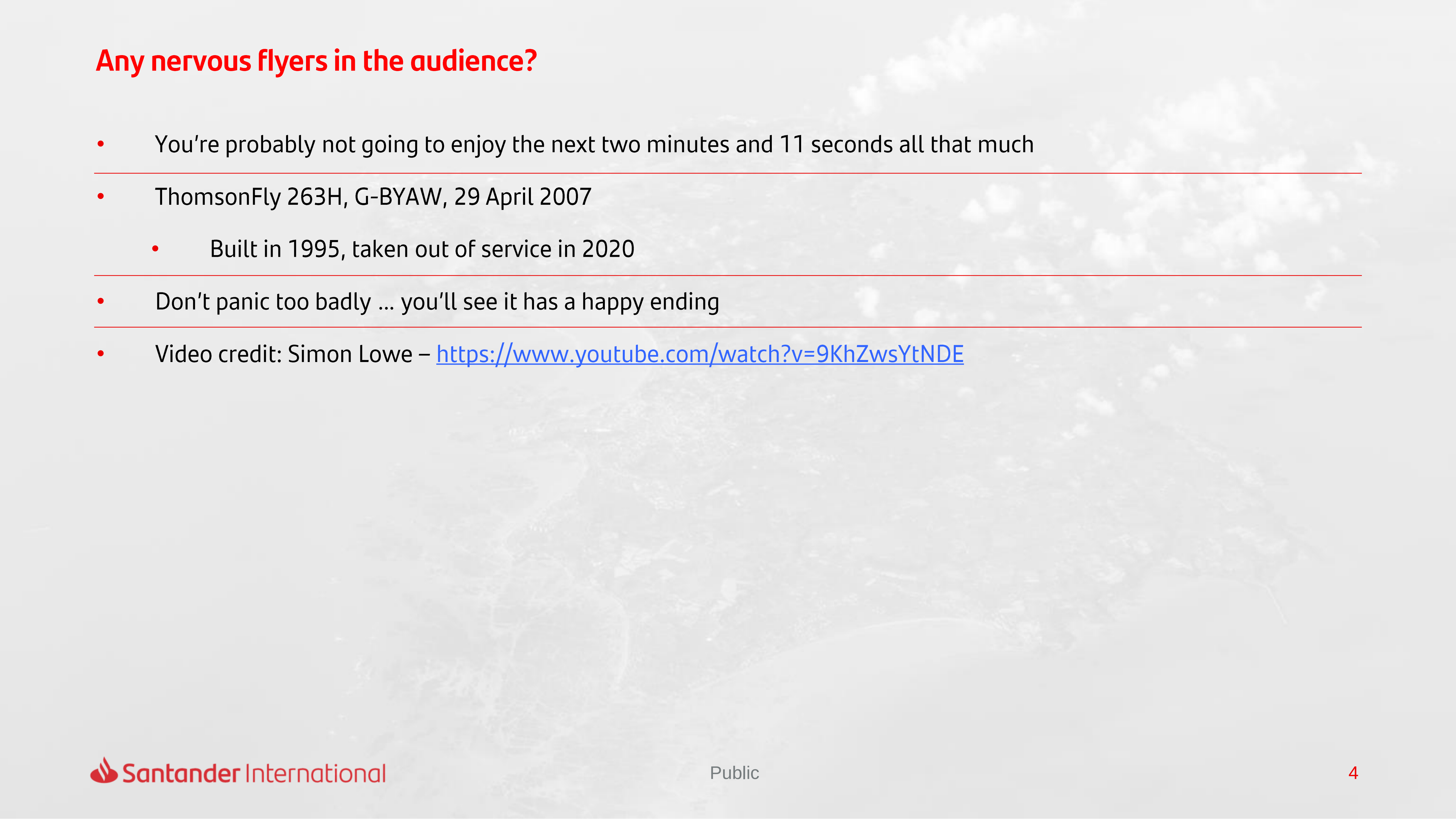
ISC2™

CISSP®

Chartered Institute of Information Security

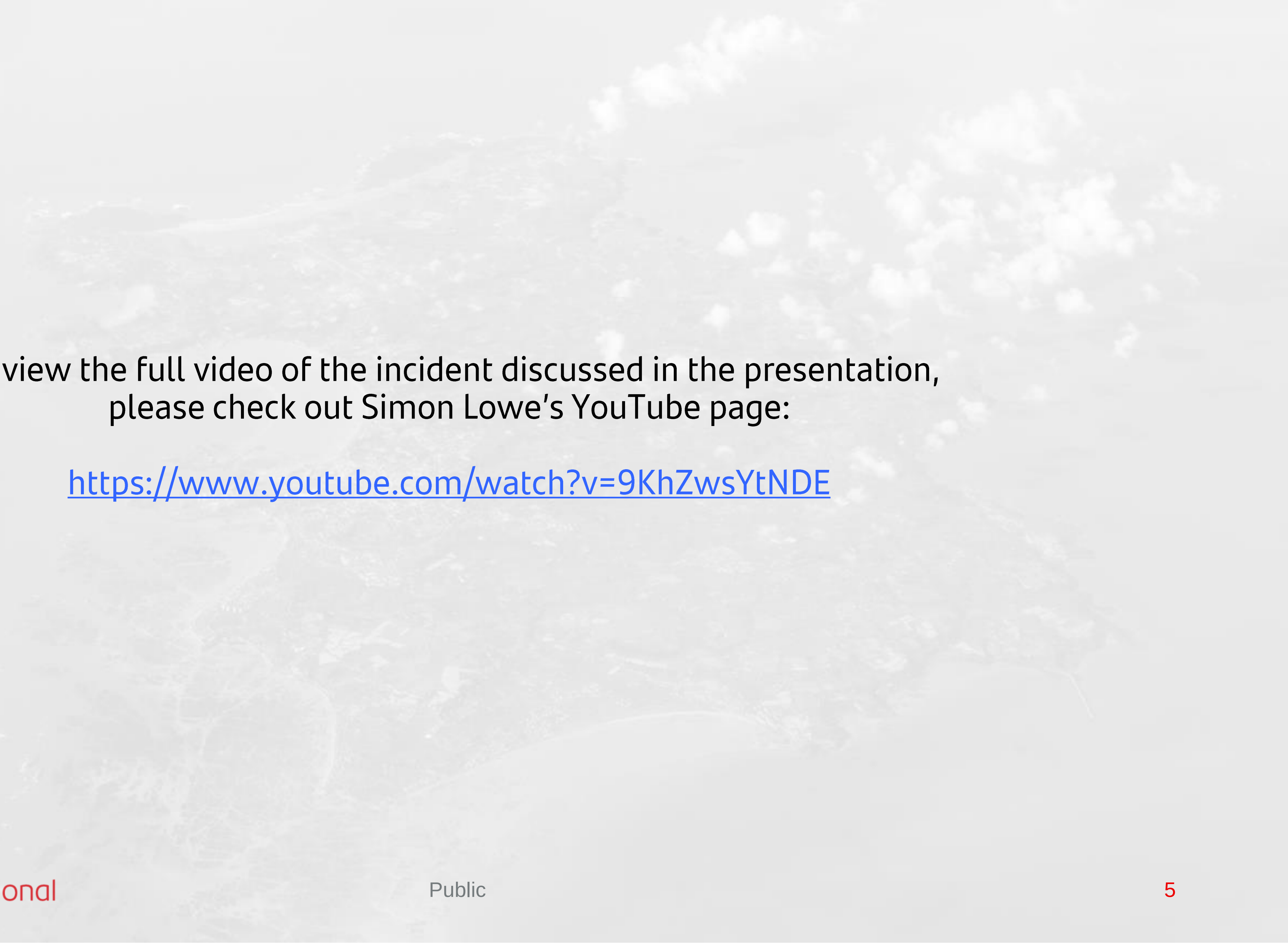
Santander International

How to do it right



Any nervous flyers in the audience?

- You’re probably not going to enjoy the next two minutes and 11 seconds all that much
- ThomsonFly 263H, G-BYAW, 29 April 2007
  - Built in 1995, taken out of service in 2020
- Don’t panic too badly … you’ll see it has a happy ending
- Video credit: Simon Lowe – https://www.youtube.com/watch?v=9KhZwsYtNDE

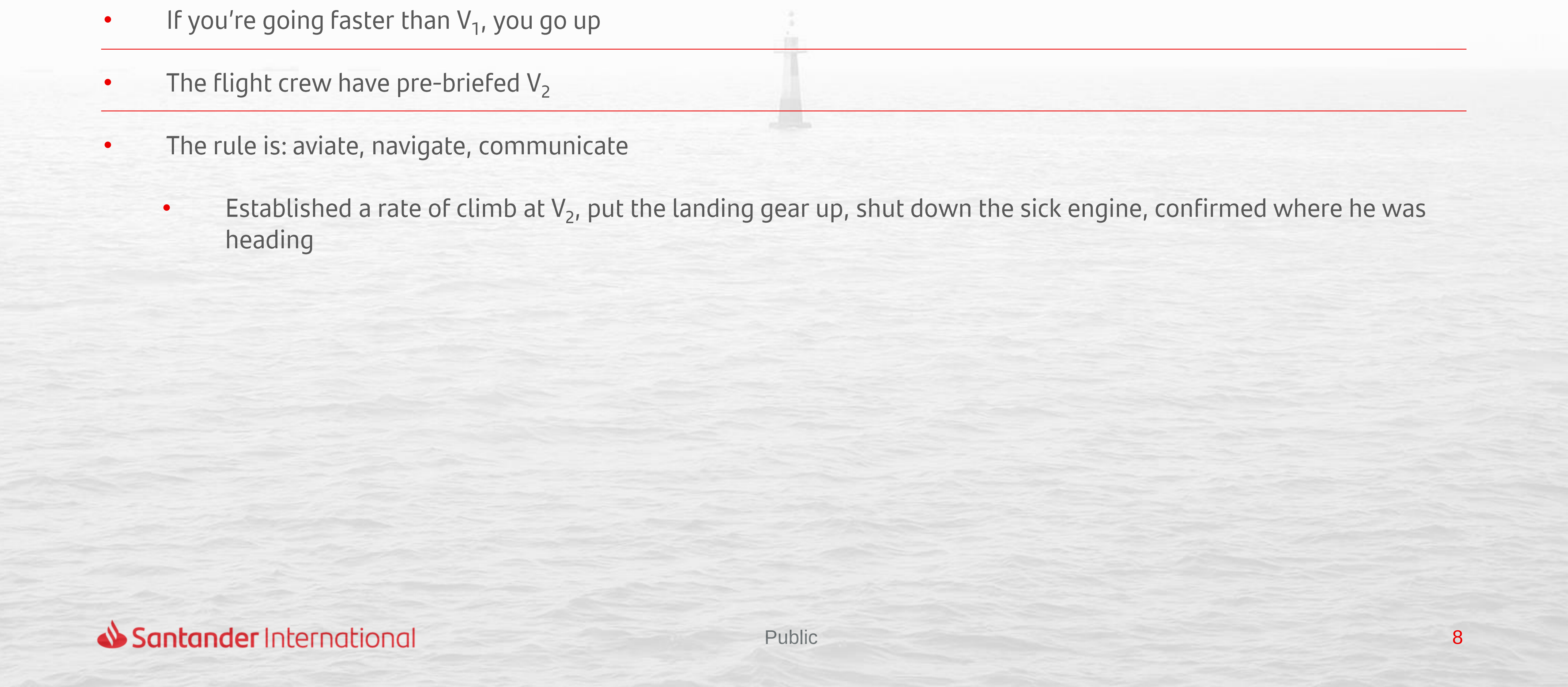


To view the full video of the incident discussed in the presentation, please check out Simon Lowe's YouTube page:

https://www.youtube.com/watch?v=9KhZwsYtNDE

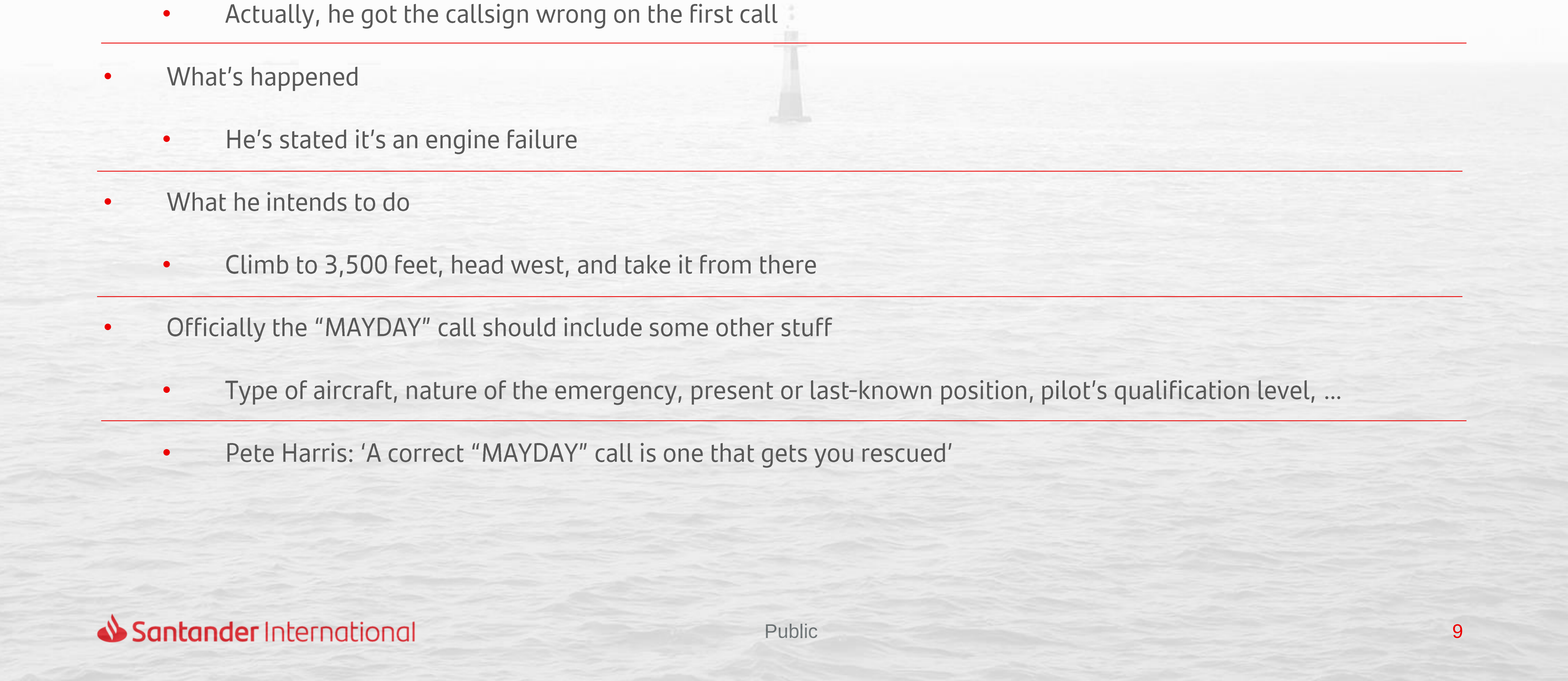
Let's look at the key points

Invoking the incident response: Deciding what to do



- Actually there's no decision to make – it's all predetermined
- If you're going faster than V_1, you go up
- The flight crew have pre-briefed V_2
- The rule is: aviate, navigate, communicate
  - Established a rate of climb at V_2, put the landing gear up, shut down the sick engine, confirmed where he was heading

Invoking the incident response: The “MAYDAY” call

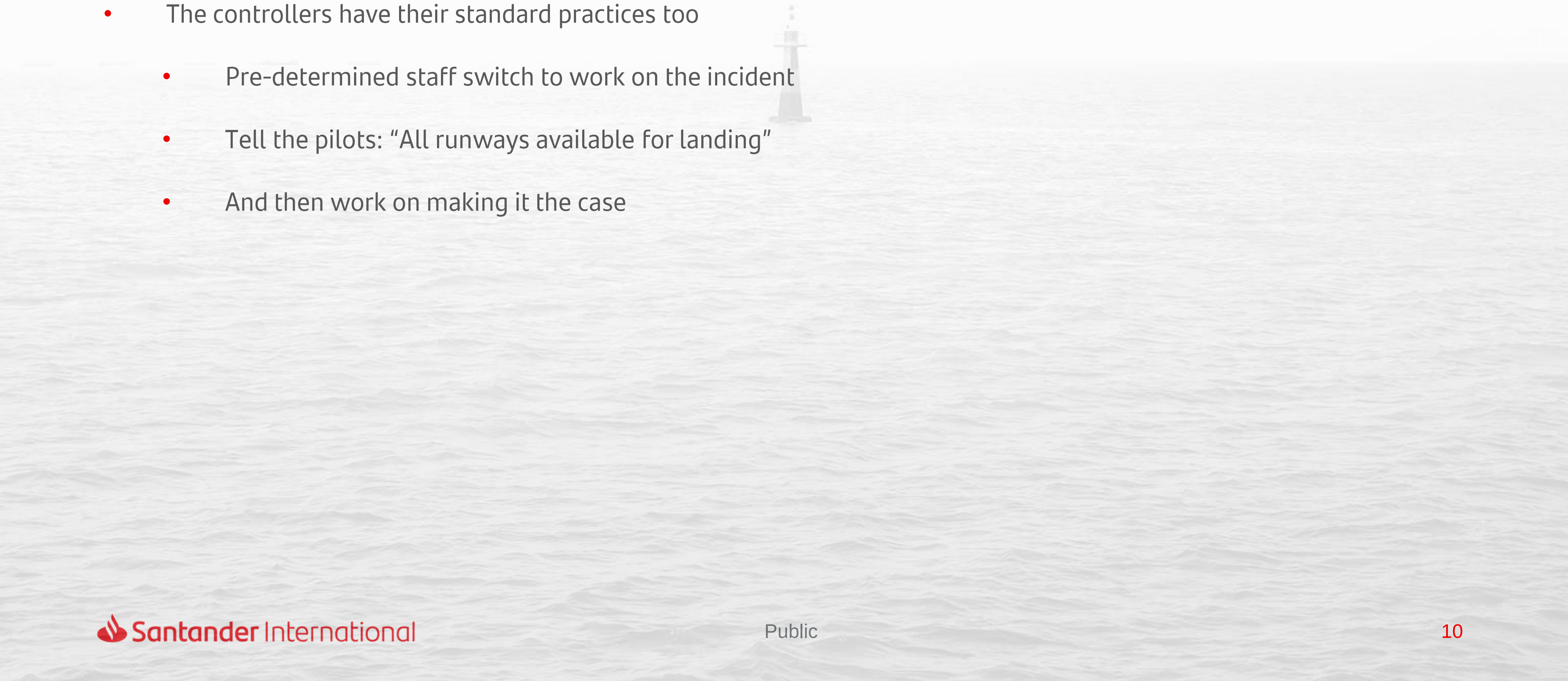


- Who he is
  - Actually, he got the callsign wrong on the first call
- What’s happened
  - He’s stated it’s an engine failure
- What he intends to do
  - Climb to 3,500 feet, head west, and take it from there
- Officially the “MAYDAY” call should include some other stuff
  - Type of aircraft, nature of the emergency, present or last-known position, pilot’s qualification level, …
  - Pete Harris: ‘A correct “MAYDAY” call is one that gets you rescued’

The controller’s response

- Acknowledged receipt of the message

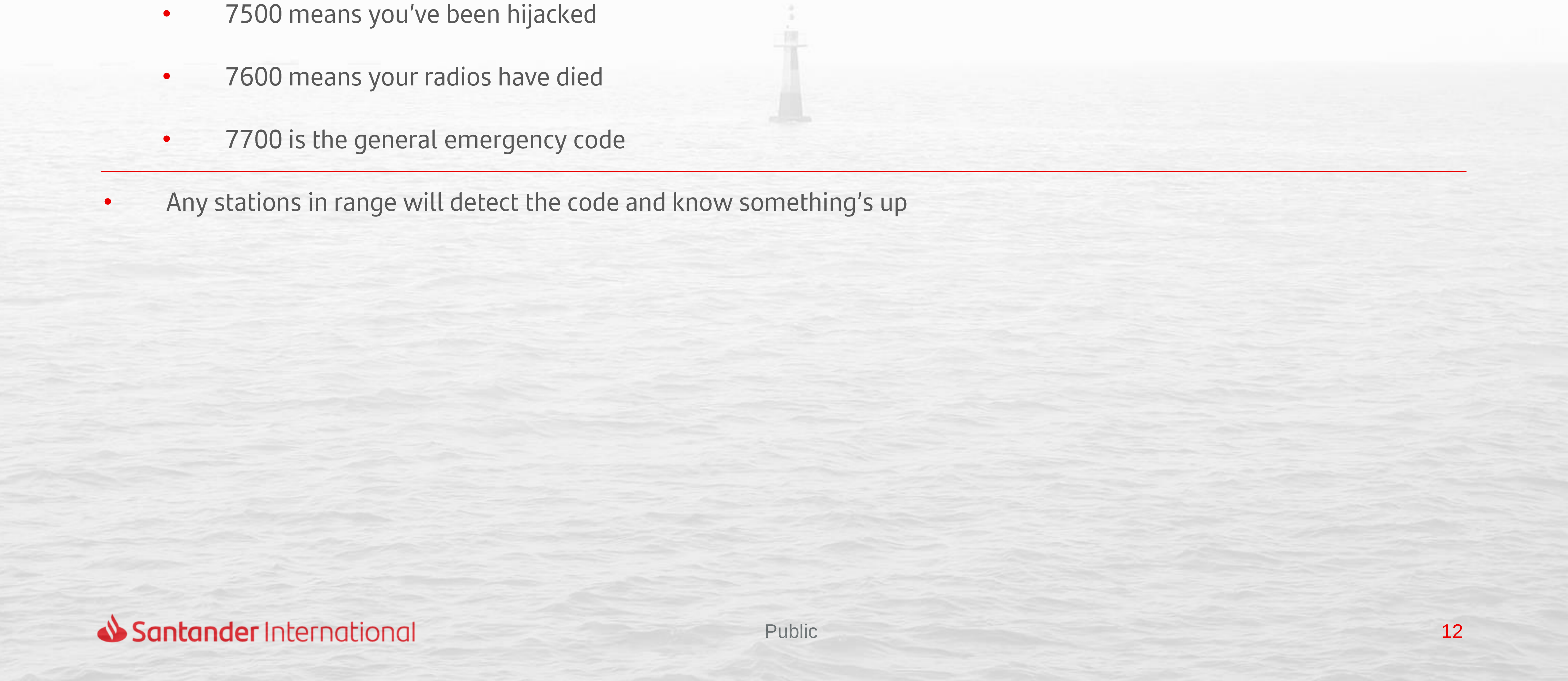
- The controllers have their standard practices too
  - Pre-determined staff switch to work on the incident
  - Tell the pilots: “All runways available for landing”
  - And then work on making it the case



As the incident continued

- Controller has already alerted his supervisor and team

- Other team members are assisting
    - Checking with other local airports (in this case Liverpool)
    - Alerting the emergency services
    - Arranging to examine the runway



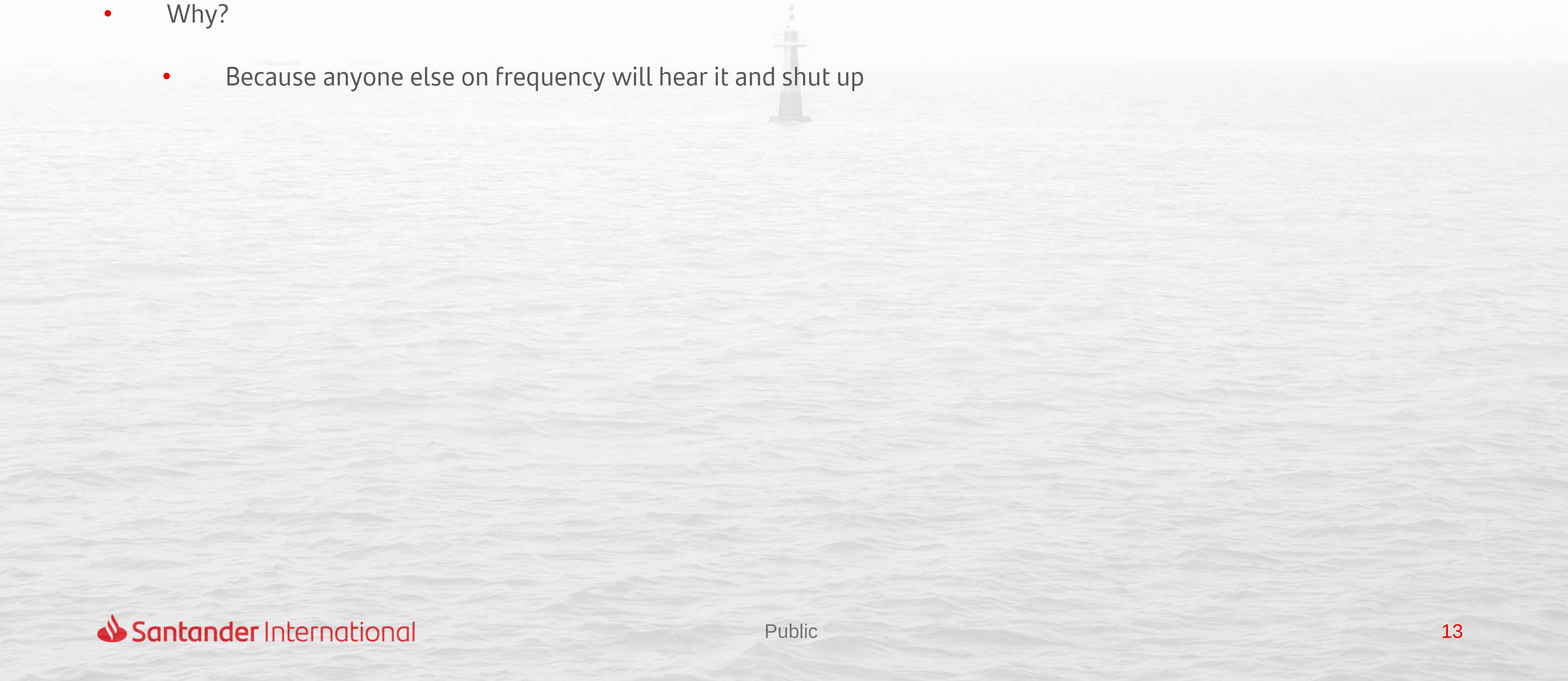
“Squawk 7700”

- “Squawk” means set the radar transponder
  - 7500 means you’ve been hijacked
  - 7600 means your radios have died
  - 7700 is the general emergency code
- Any stations in range will detect the code and know something’s up

Why is he calling himself that: *Mayday* Thomson 263H?

- Standard practice to start radio calls with “Mayday”

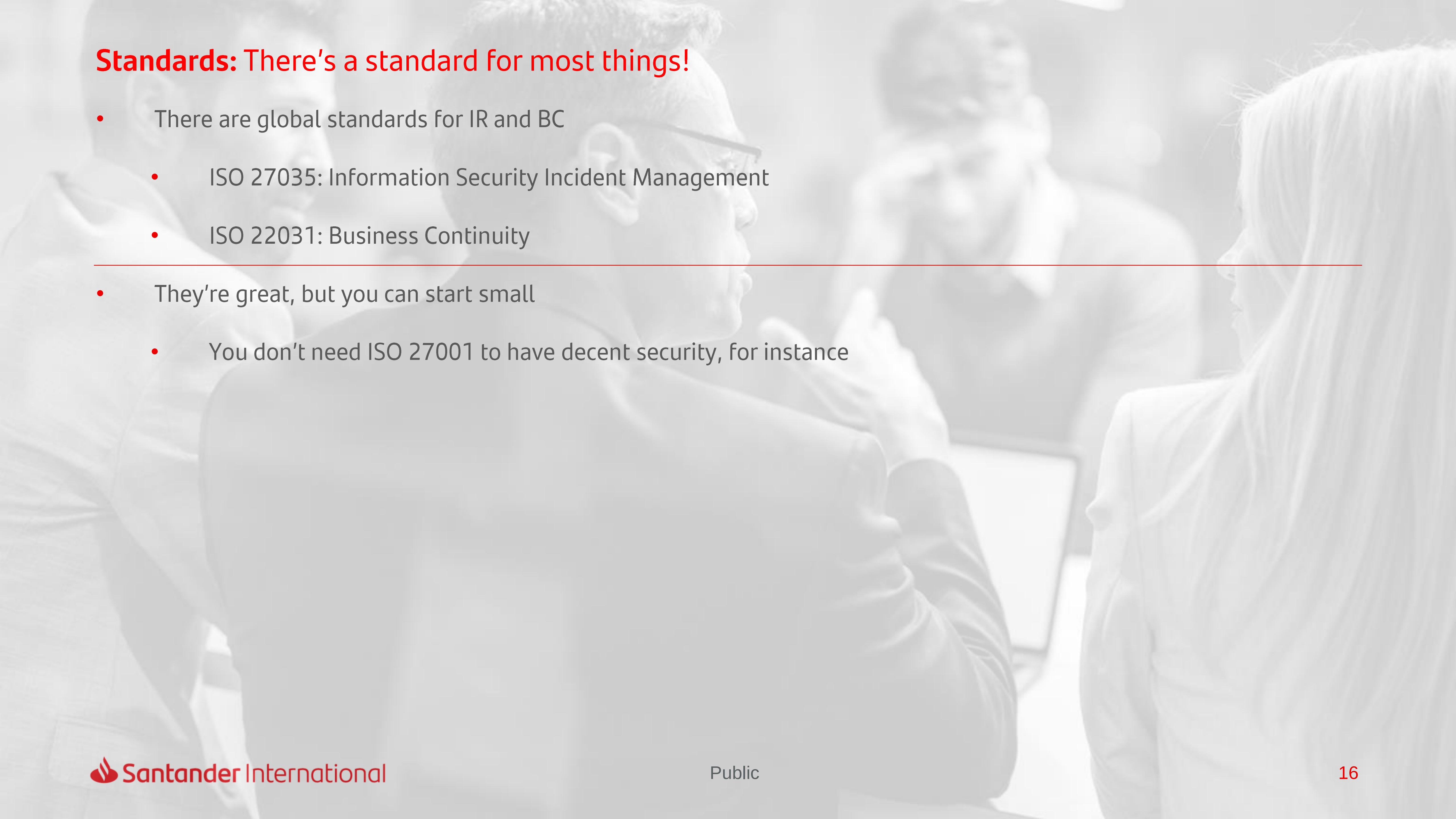
- Why?
  - Because anyone else on frequency will hear it and shut up



“Emergency, which service?”: All of them, please

- Airfield fire service and local fire service attended
- Emergency services will always try to over-deliver people and equipment
- AFS is mobilised simply by operating a “crash alarm” at many airfields

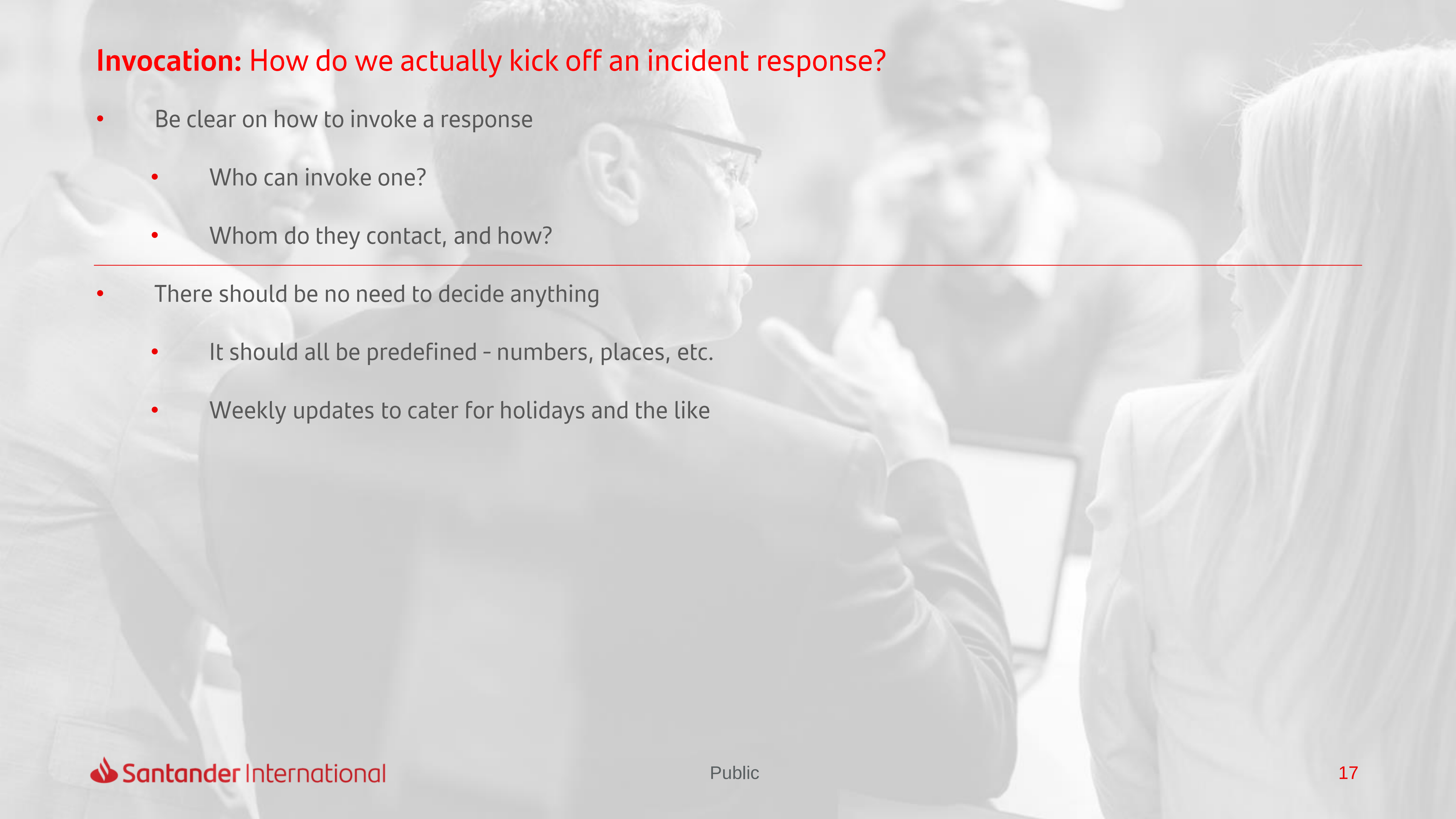
How do we map this onto our own organisations?



Standards: There’s a standard for most things!

- There are global standards for IR and BC
  - ISO 27035: Information Security Incident Management
  - ISO 22031: Business Continuity

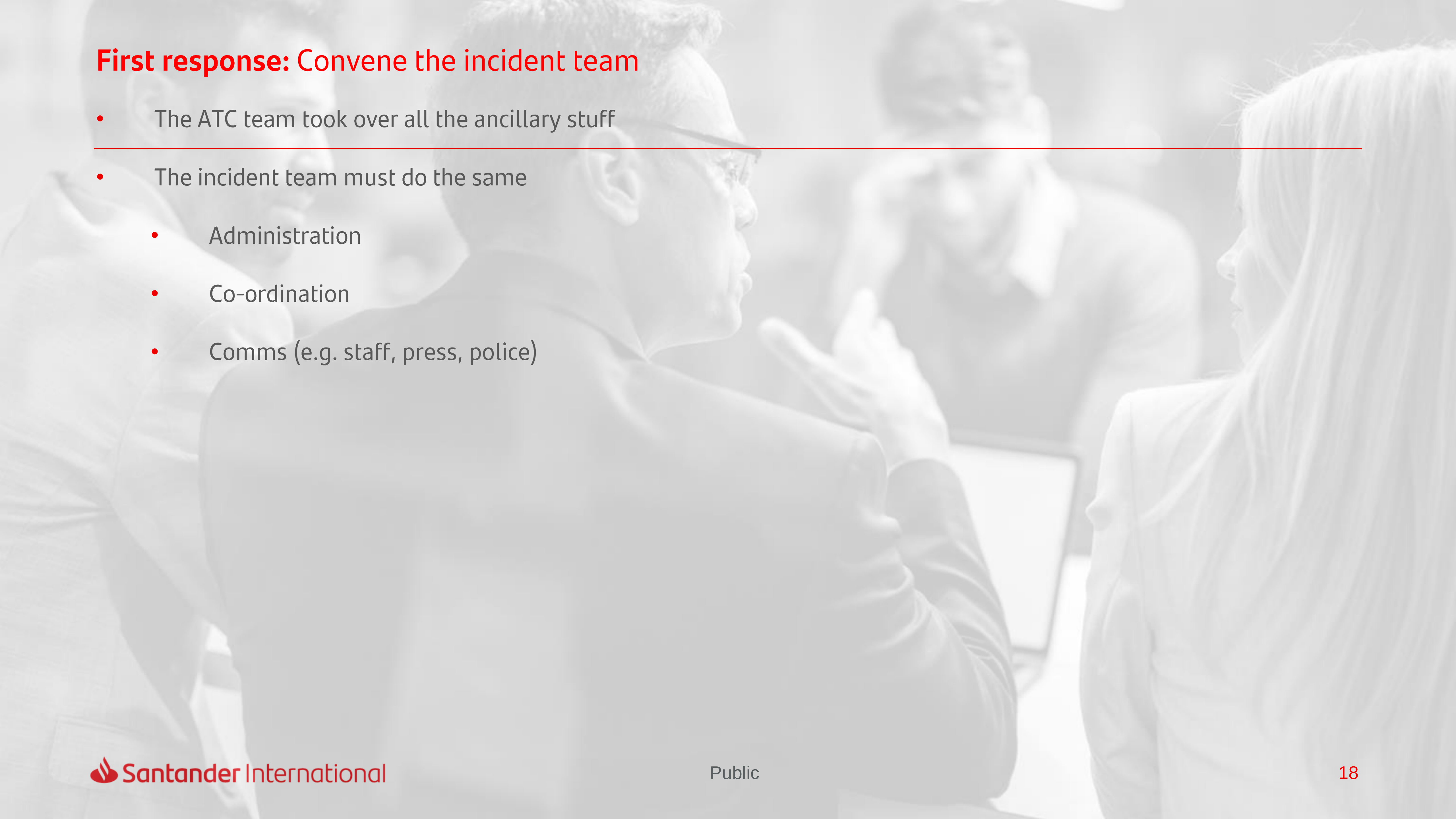
- They’re great, but you can start small
  - You don’t need ISO 27001 to have decent security, for instance



Invocation: How do we actually kick off an incident response?

- Be clear on how to invoke a response
  - Who can invoke one?
  - Whom do they contact, and how?

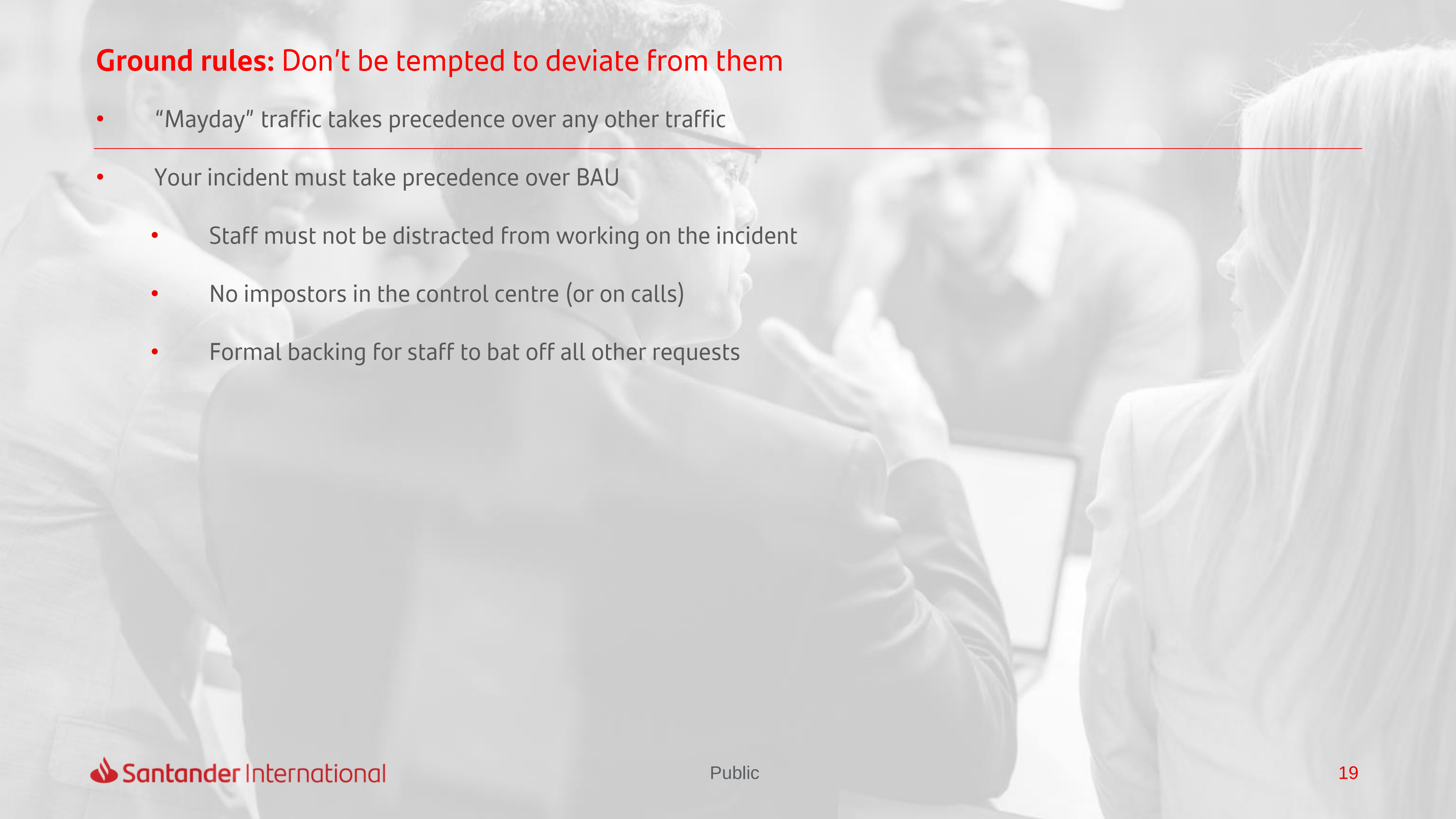
- There should be no need to decide anything
  - It should all be predefined - numbers, places, etc.
  - Weekly updates to cater for holidays and the like



First response: Convene the incident team

- The ATC team took over all the ancillary stuff

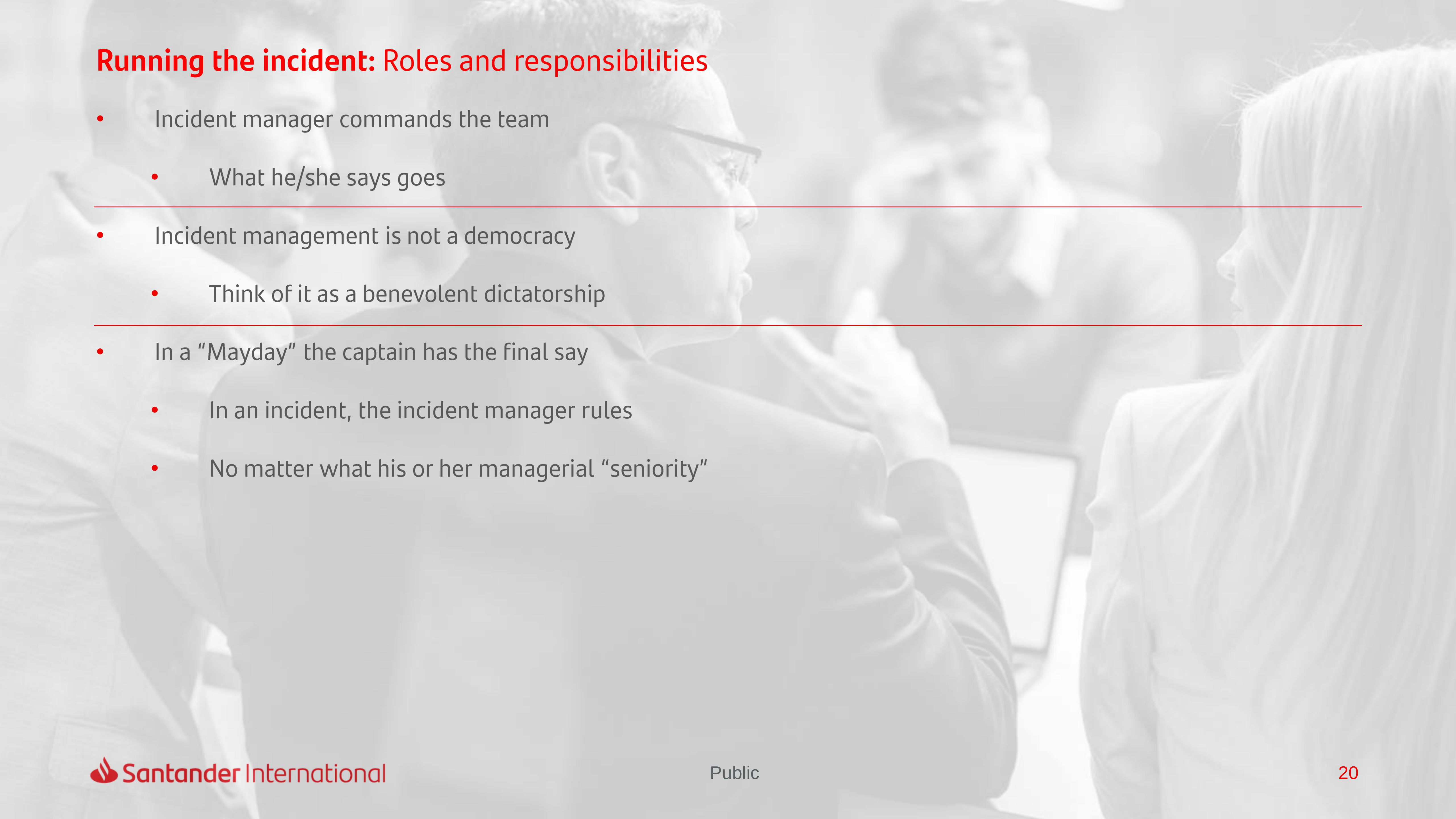
- The incident team must do the same
  - Administration
  - Co-ordination
  - Comms (e.g. staff, press, police)



Ground rules: Don’t be tempted to deviate from them

- “Mayday” traffic takes precedence over any other traffic

- Your incident must take precedence over BAU
  - Staff must not be distracted from working on the incident
  - No impostors in the control centre (or on calls)
  - Formal backing for staff to bat off all other requests

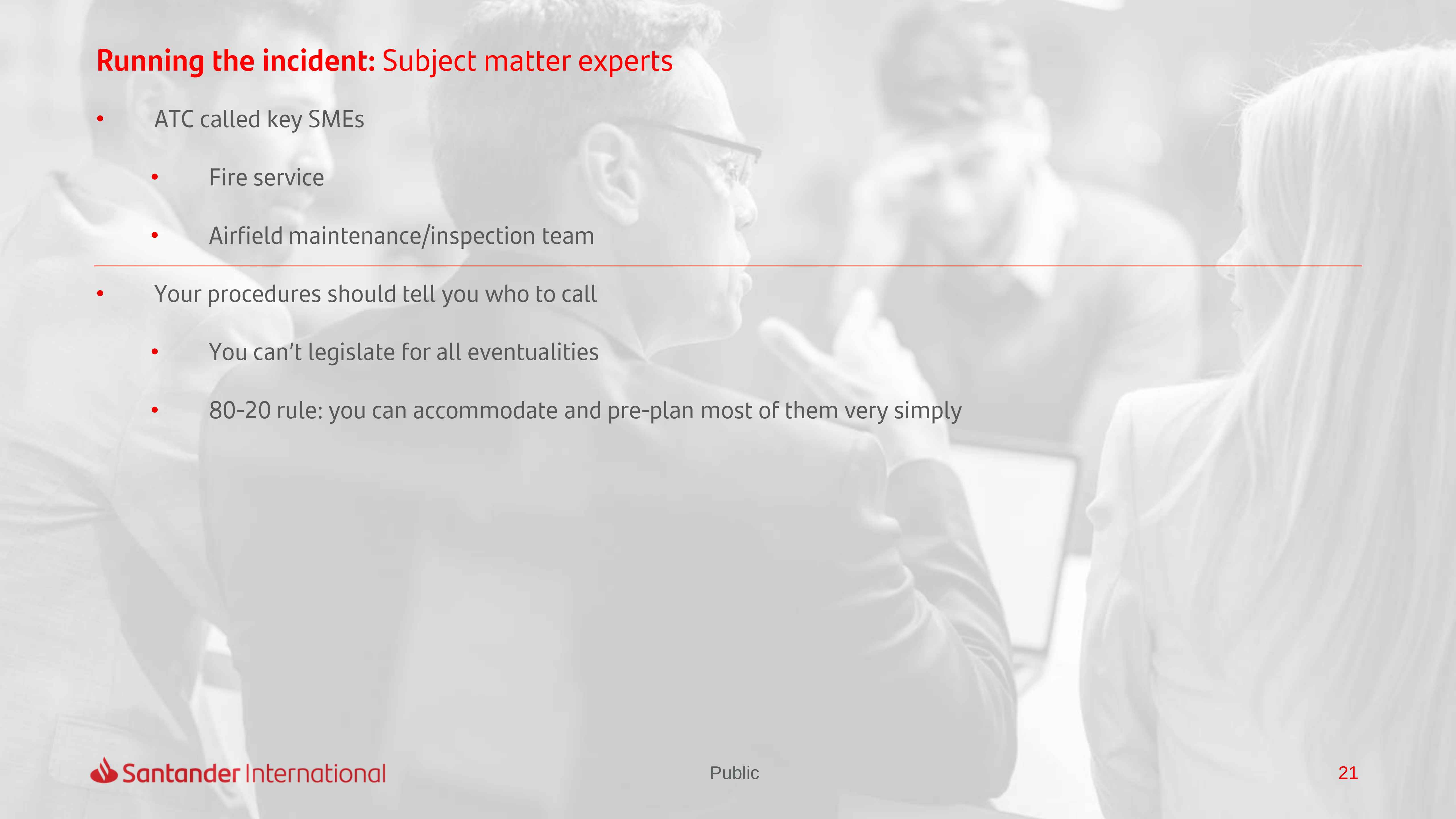


Running the incident: Roles and responsibilities

- Incident manager commands the team
  - What he/she says goes

- Incident management is not a democracy
  - Think of it as a benevolent dictatorship

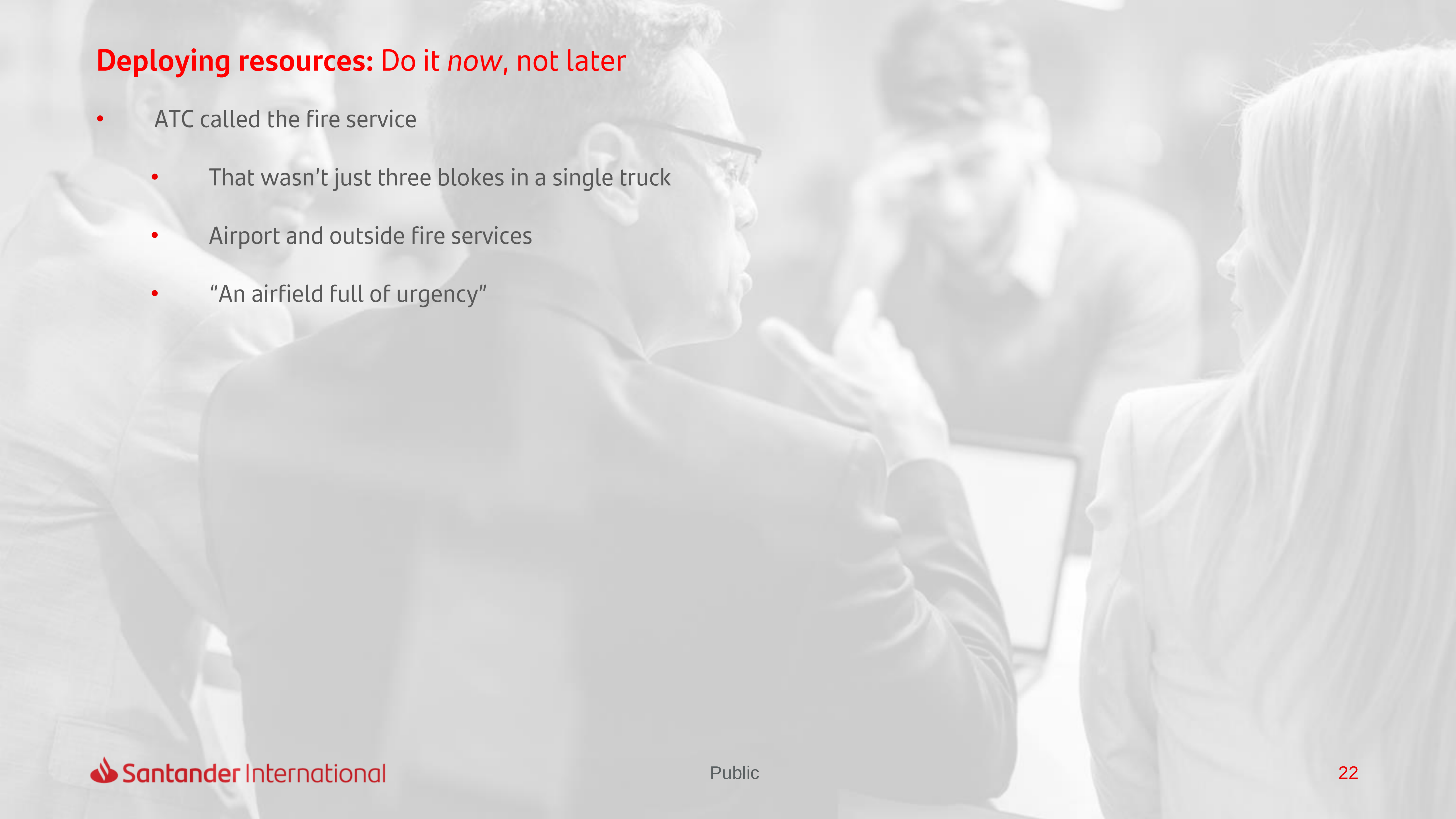
- In a “Mayday” the captain has the final say
  - In an incident, the incident manager rules
  - No matter what his or her managerial “seniority”



Running the incident: Subject matter experts

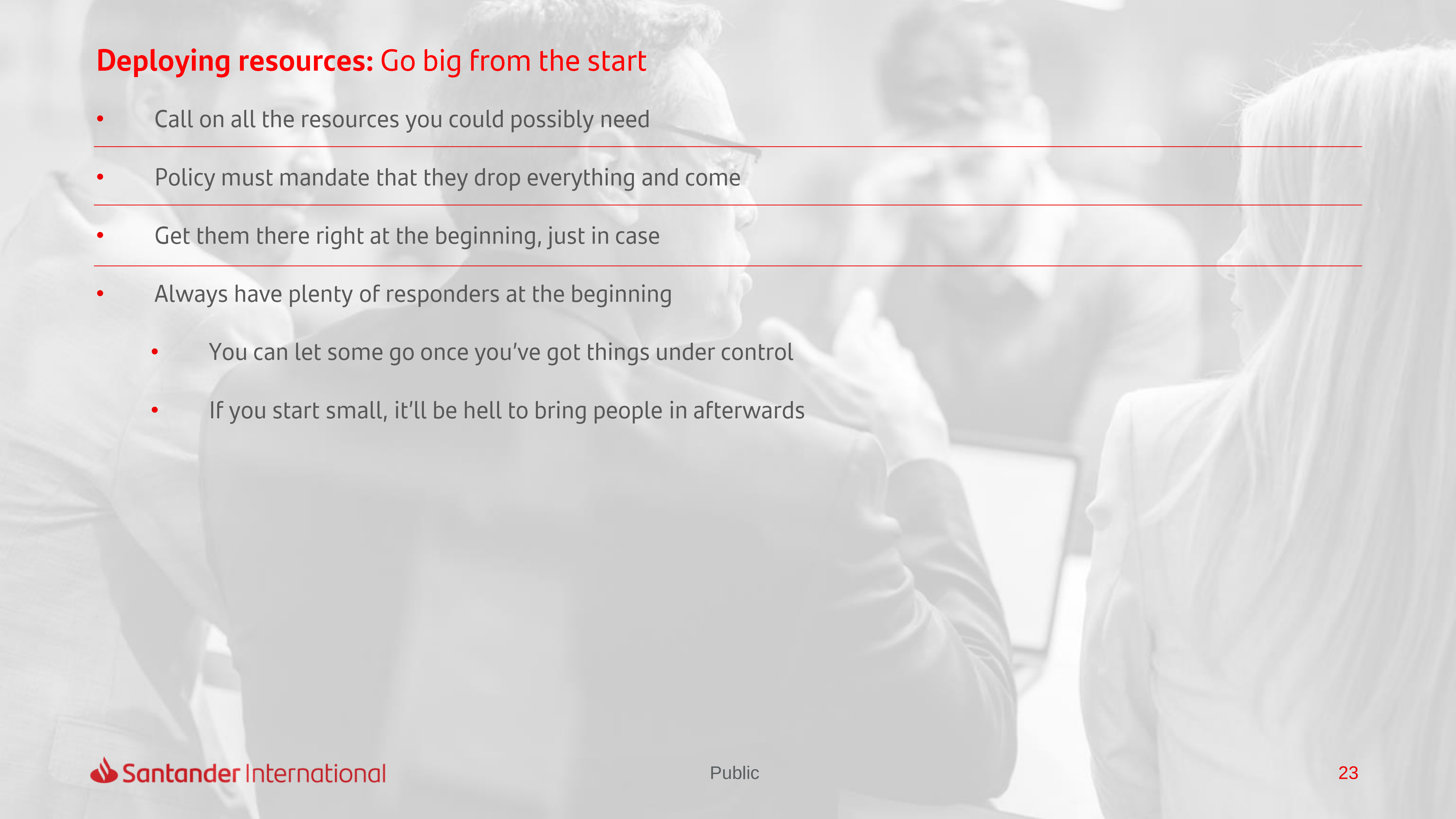
- ATC called key SMEs
  - Fire service
  - Airfield maintenance/inspection team

- Your procedures should tell you who to call
  - You can't legislate for all eventualities
  - 80-20 rule: you can accommodate and pre-plan most of them very simply



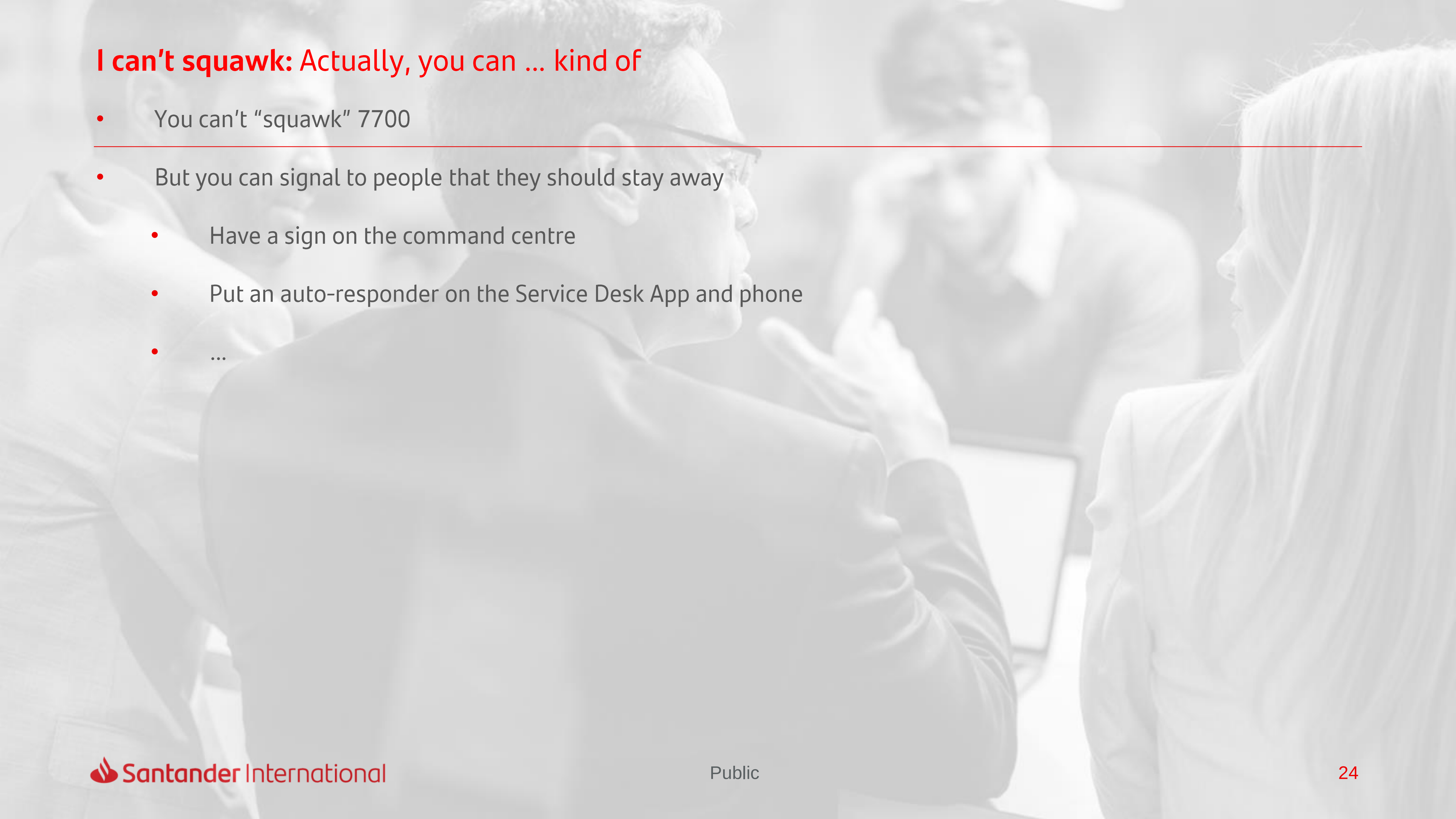
Deploying resources: Do it *now*, not later

- ATC called the fire service
  - That wasn't just three blokes in a single truck
  - Airport and outside fire services
  - "An airfield full of urgency"



Deploying resources: Go big from the start

- Call on all the resources you could possibly need
- Policy must mandate that they drop everything and come
- Get them there right at the beginning, just in case
- Always have plenty of responders at the beginning
  - You can let some go once you've got things under control
  - If you start small, it'll be hell to bring people in afterwards

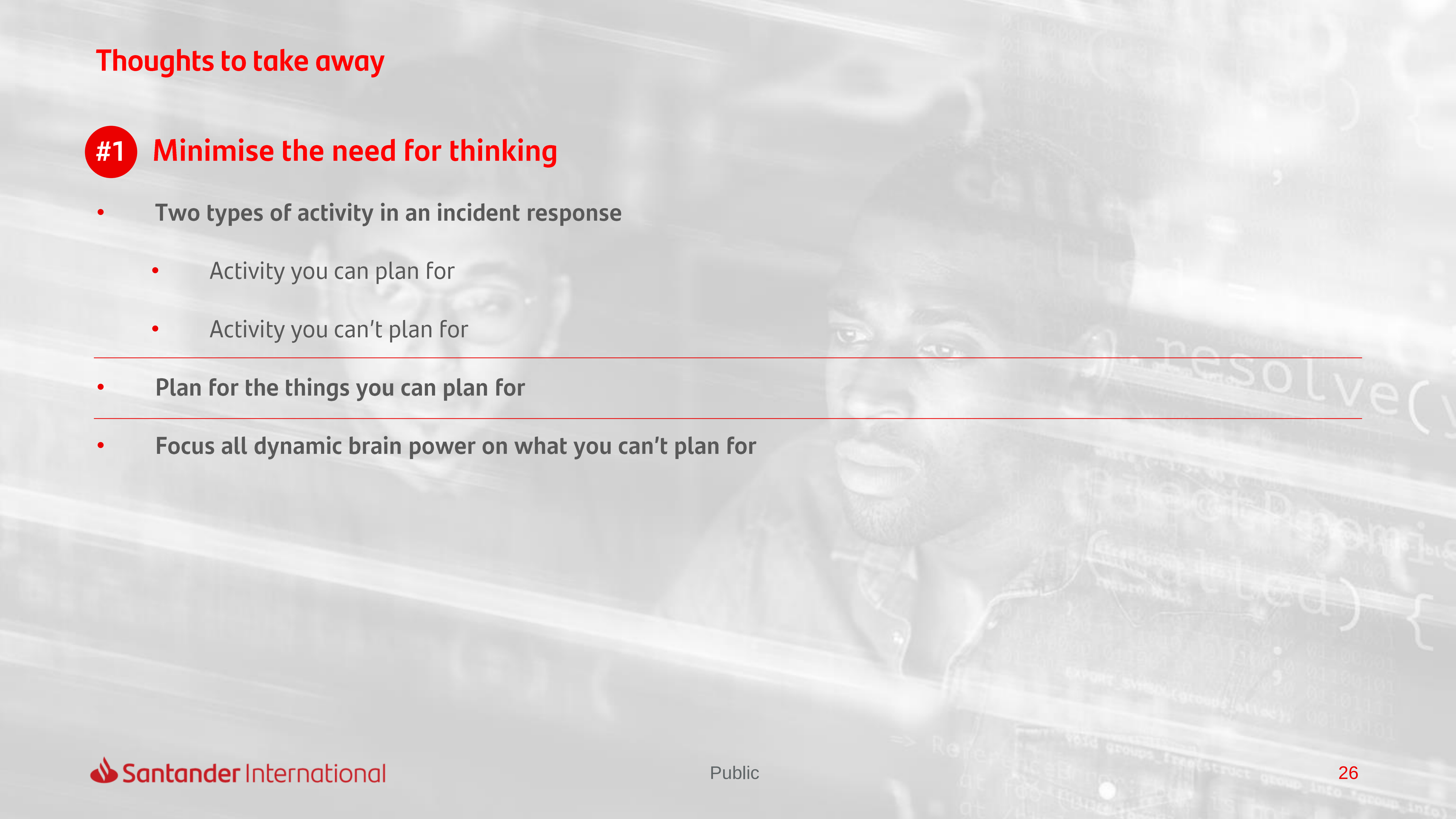


I can’t squawk: Actually, you can … kind of

- You can’t “squawk” 7700

- But you can signal to people that they should stay away
  - Have a sign on the command centre
  - Put an auto-responder on the Service Desk App and phone
  - …

Three thoughts to take home with you



Thoughts to take away

#1 Minimise the need for thinking

- **Two types of activity in an incident response**
  - Activity you can plan for
  - Activity you can't plan for
- **Plan for the things you can plan for**
- **Focus all dynamic brain power on what you can't plan for**

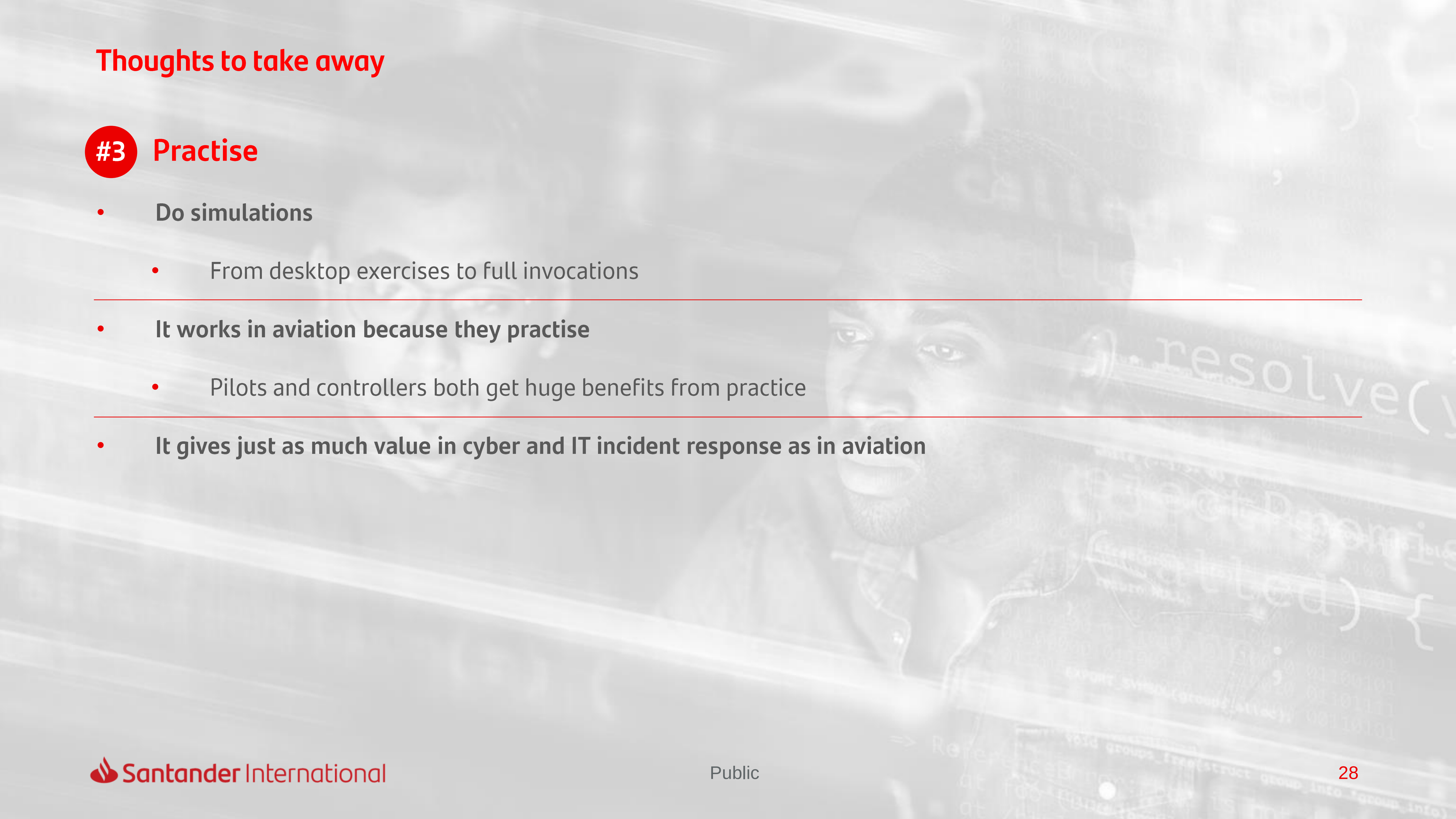
Thoughts to take away

#2 Have teams to work on the incident

- **One call mobilises a pre-ordained internal team**

- **Call other internal teams where they’re required**
  - And make sure they’re always expecting your call

- **Call external teams when they’re required**
  - And make sure they’re always expecting your call



Thoughts to take away

#3 Practise

- **Do simulations**
  - From desktop exercises to full invocations

- **It works in aviation because they practise**
  - Pilots and controllers both get huge benefits from practice

- **It gives just as much value in cyber and IT incident response as in aviation**

Santander International

Thank you.

Feel free to get in touch:

- linkedin.com/in/davidscartwright/
- @DaveTheCISO
- David.Cartwright@santanderinternational.co.uk

MEMBER OF
Dow Jones
Sustainability Indices
In Collaboration with RobecoSAM

FTSE4Good