

RSA[®]Conference2022

San Francisco & Digital | June 6 – 9

SESSION ID: HUM-R02

Lessons From Aviation: Building a Just Culture in Cybersecurity

John Elliott

Consultant and Pluralsight Author

@withoutfire

TRANSFORM



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.



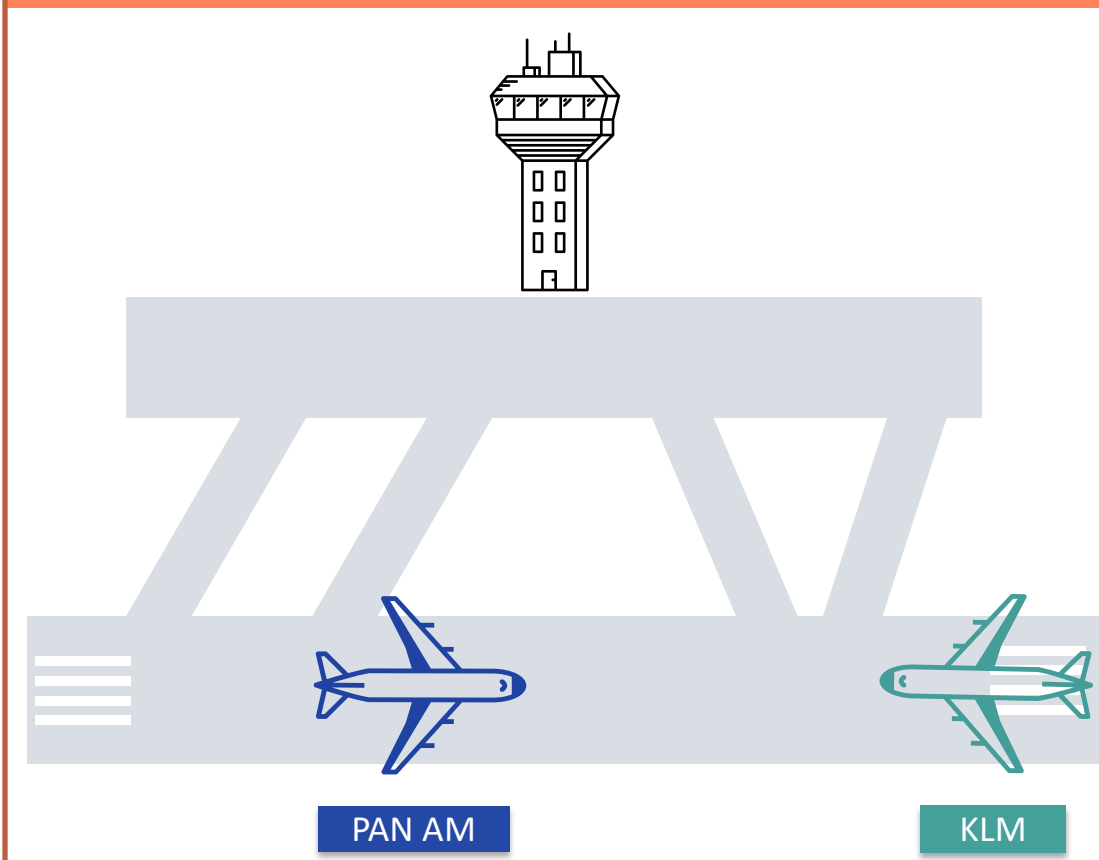
What happened in aviation in the 1970s?



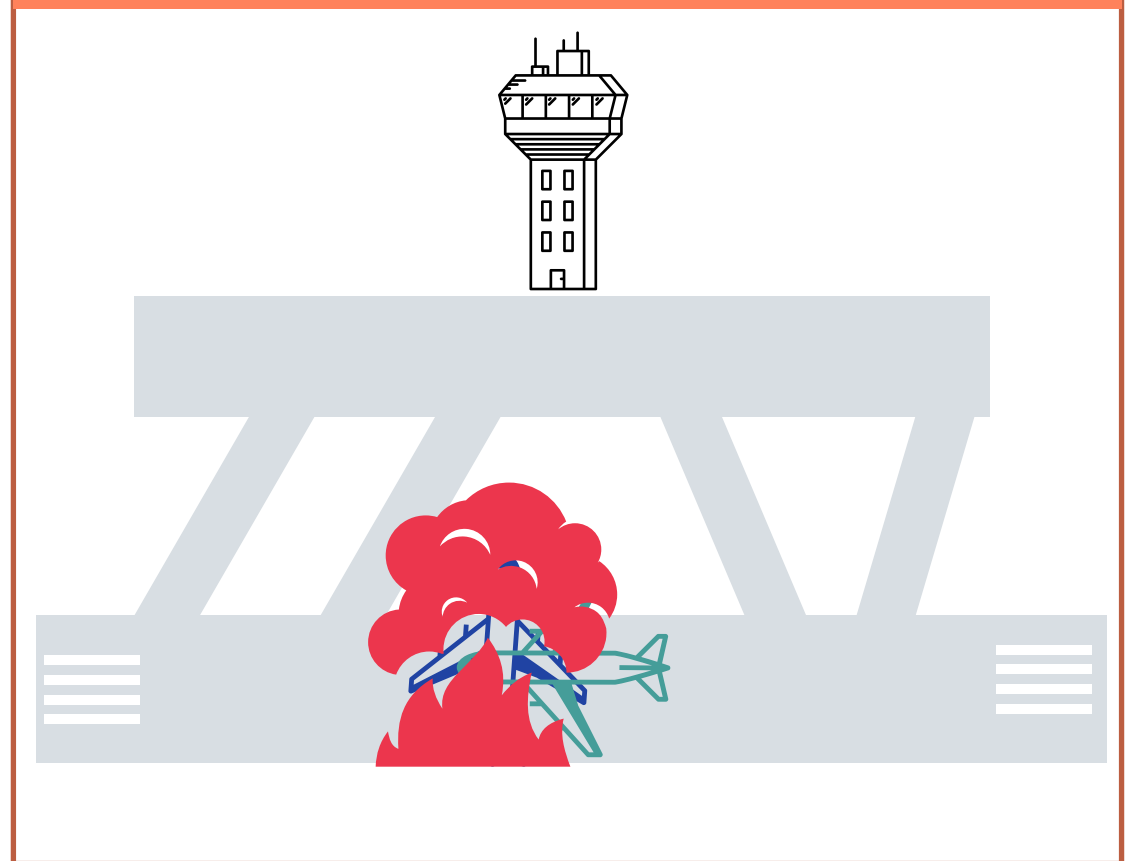
- Number of commercial airlines and flights increasing
 - Deregulation
- Number of accidents increasing
- Number of fatalities increasing
- Flying perceived to be less safe
- Government regulation

Tenerife Airport Disaster

How it started



How it finished



What was the cause of the accident?

Human
failure?

Systems
failure?

Contributory factors

- Pilot's actions ← Human failure
- Engineer's actions ← Human failure
- Air Traffic Control (ATC) actions ← Human failure

Key Lessons

- Pilot's actions ← Human failure
- Engineer's actions ← Human failure
- ATC actions ← Human failure
- No ground radar and too many planes ← Systems failure
- Communications protocols ← Systems failure
- Cockpit protocols ← Systems failure

What type of human failure?

Human
Error?

At-risk
behavior?

Reckless?

Deliberate
Harm?

What Type of Human Failure?

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

RSA[®]Conference2022

How The Brain Works

And how that relates to risk



The Brain



Two Brains



System 1



System 2

System 1



- Automatic processing
- Emotional responses
- Fast!
- Multi-tasking
- “unconscious”
- Really bad at making risk decisions



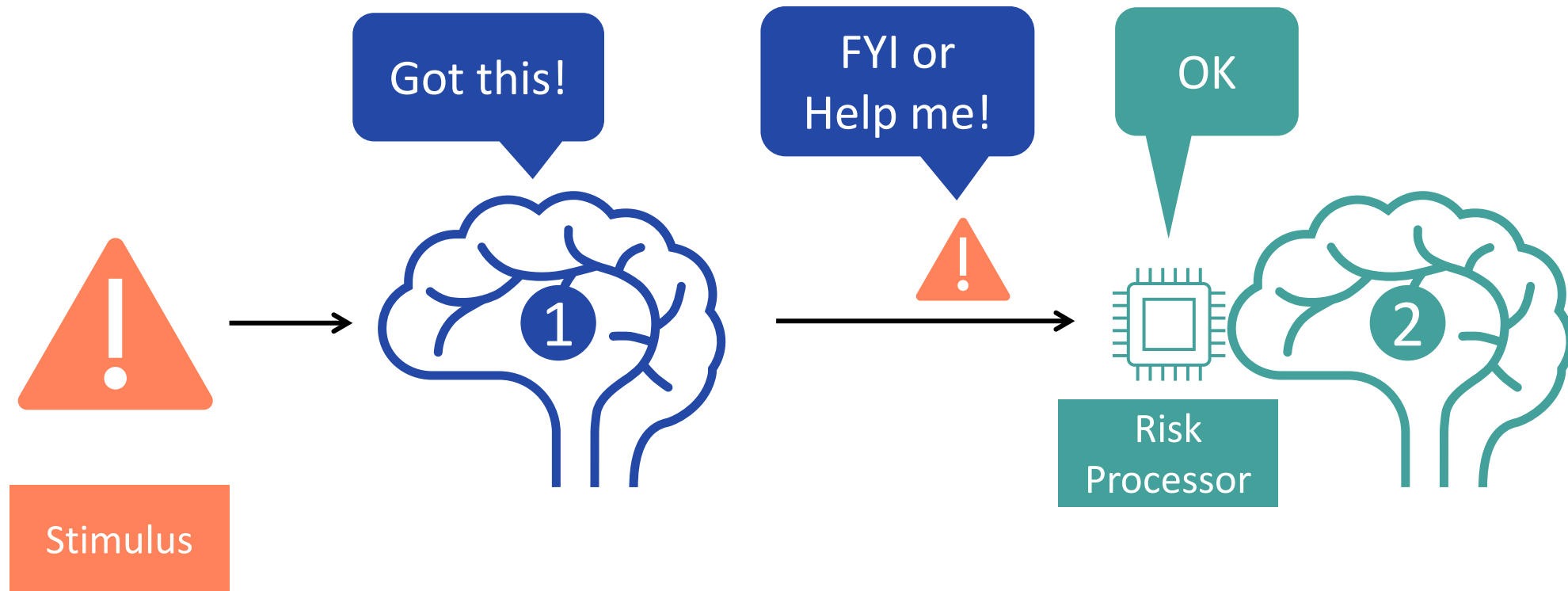
System 2



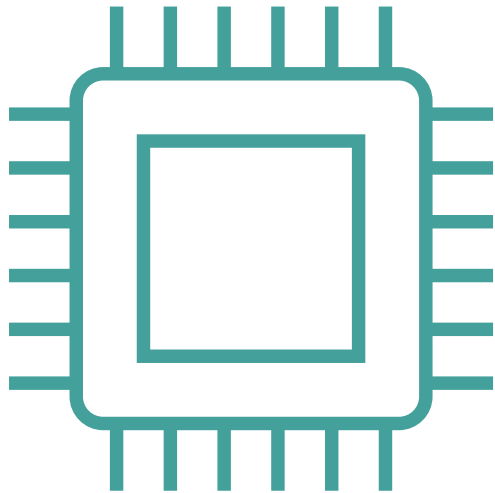
- Logical processing
- Slow
- Lazy
- Single-tasking
- “conscious”
- Better at making risk decisions



How They Communicate

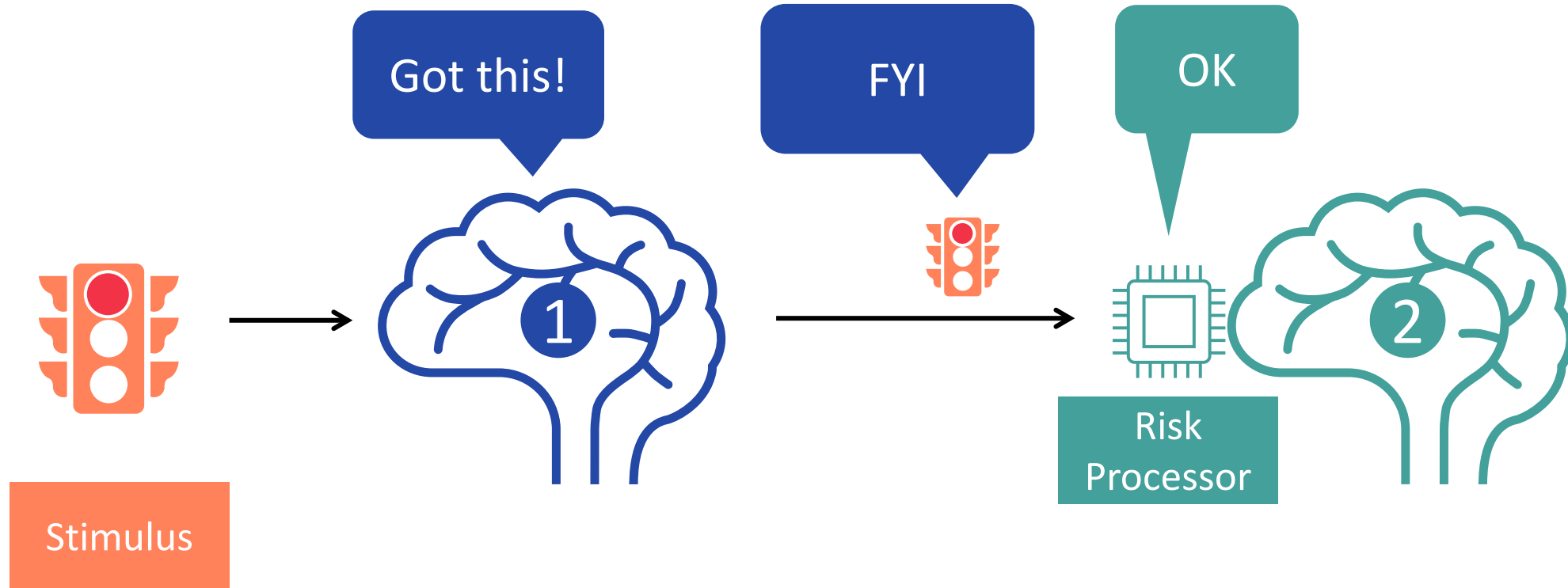


Risk Processor

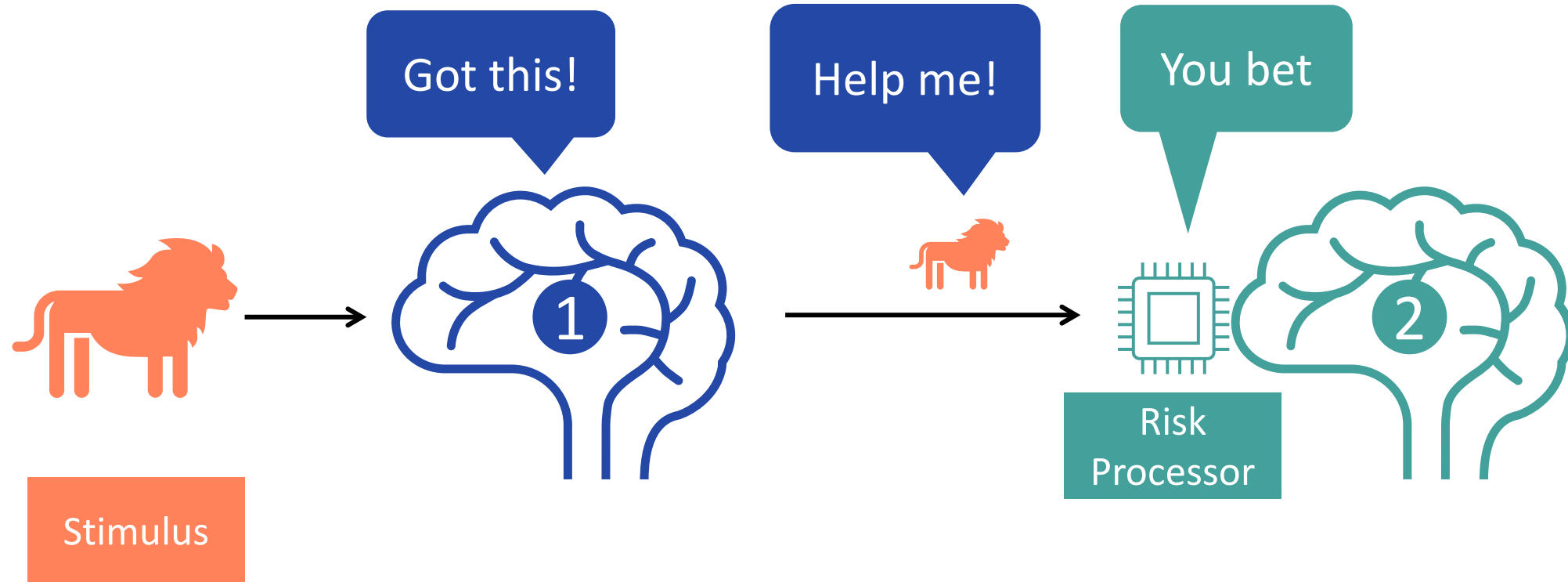


- Part of System 2
- Evaluates input from System 1
- Works out if System 2 needs to be engaged
- Trainable (AI and ML)

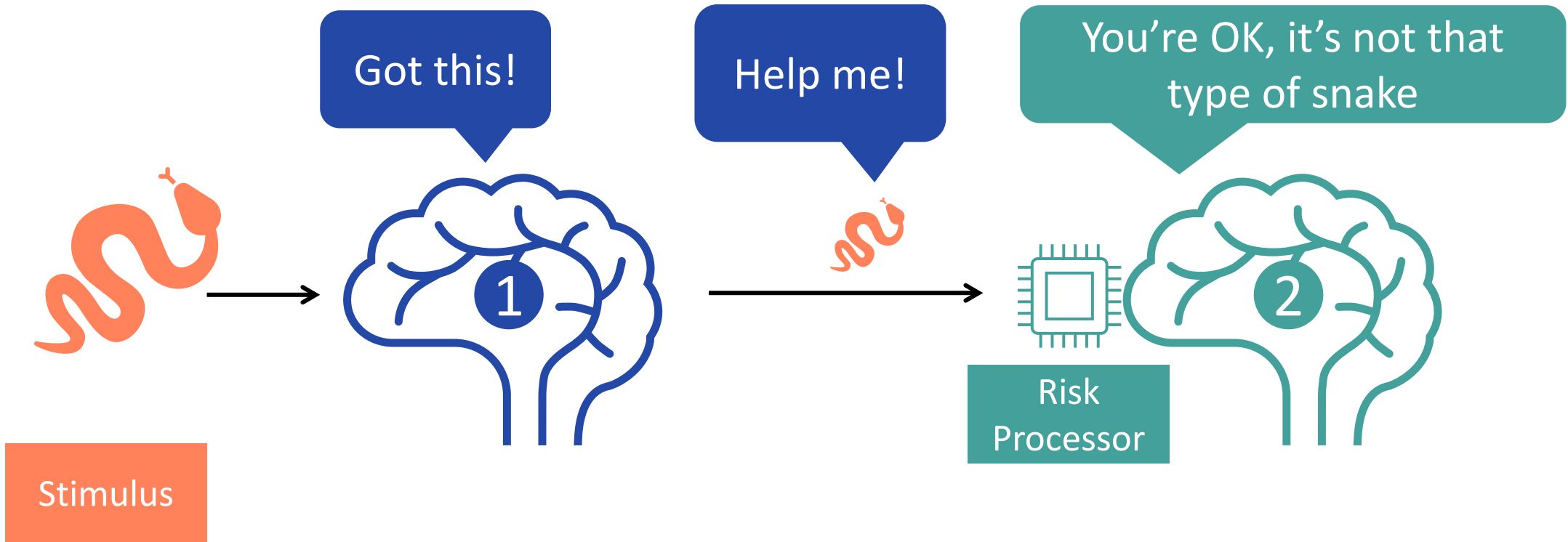
How They Communicate



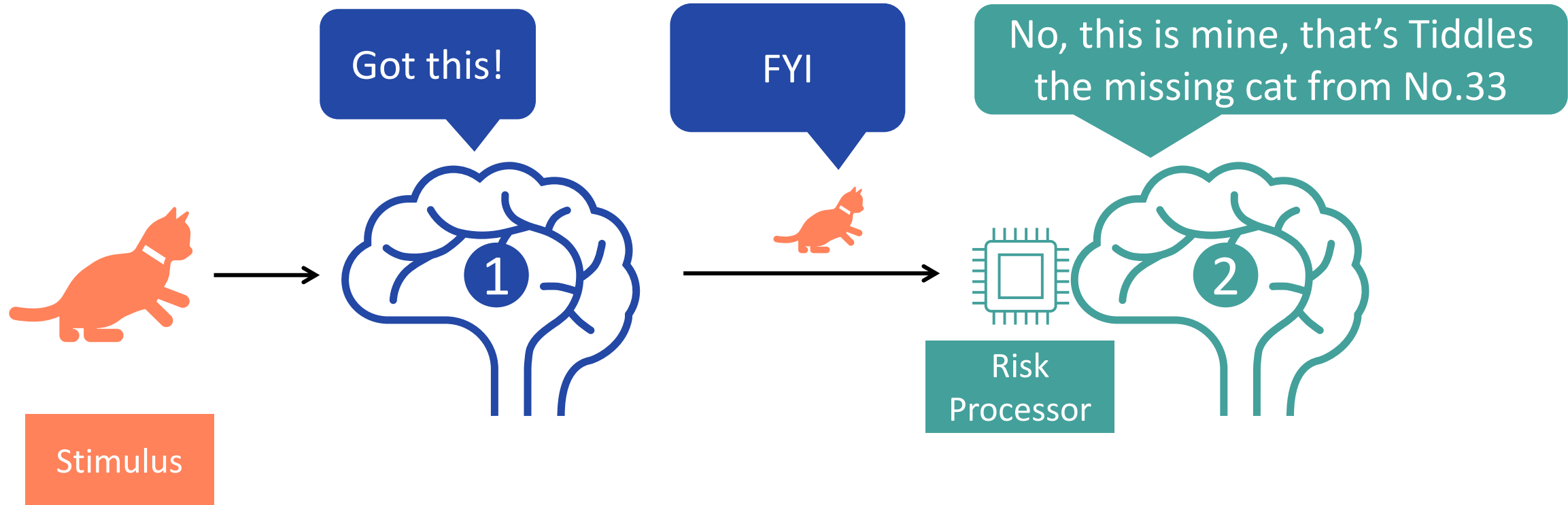
How They Communicate



How They Communicate



How They Communicate



What Type of Human Failure?

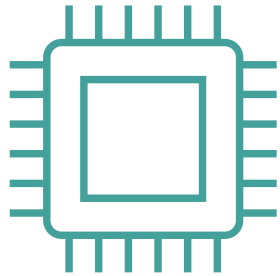
Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Used the risk

What Type of Human Failure?



OK

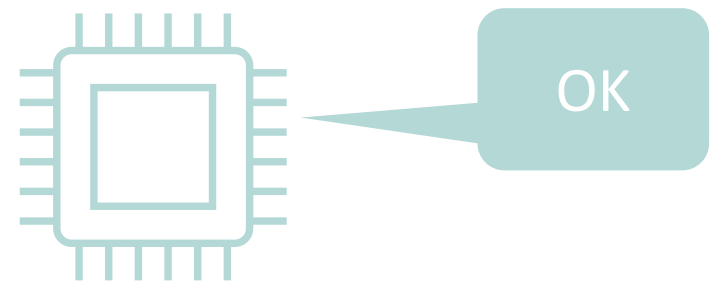
Didn't register the risk

Misinterpreted
the risk

Ignored
the risk

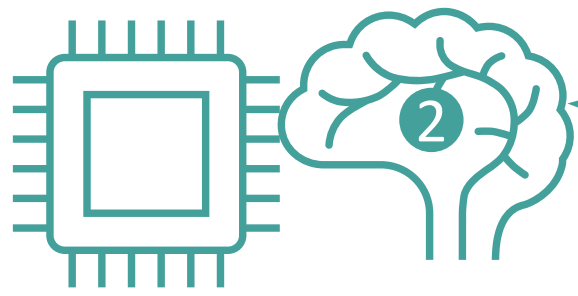
Used the risk

What Type of Human Failure?



Didn't register the risk

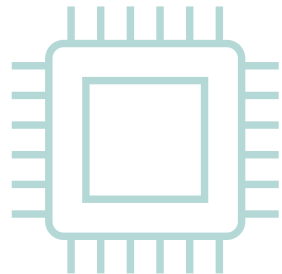
Ignored
the risk



Misinterpreted the risk

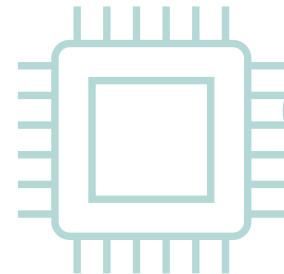
Maliciously
used the risk

What Type of Human Failure?



OK

Mine

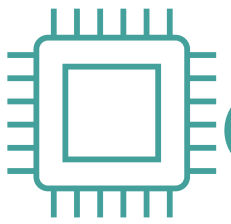


It's within appetite

Didn't register the risk

Misinterpreted the risk

Mine

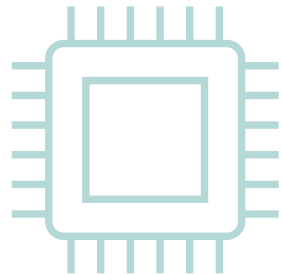


It's outside appetite, but hey

Ignored the risk

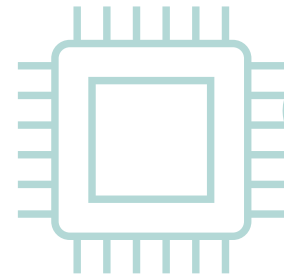
Maliciously used the risk

What Type of Human Failure?



OK

Mine

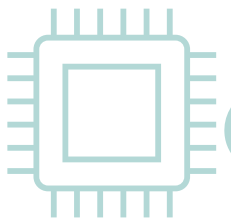


It's within appetite

Didn't register the risk

Misinterpreted the risk

Mine



It's outside appetite, but hey

Ignored the risk



Welcome to my evil plan







Maliciously used the risk

RSA®Conference2022

Back to Tenerife



Contributory factors

- Pilot's actions  Human failure
- Engineer's actions  Human failure
- ATC actions  Human failure
- No ground radar and too many planes  Systems failure
- Communications protocols  Systems failure
- Cockpit protocols  Systems failure

What type of human failure?

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Used the risk

What type of human failure?

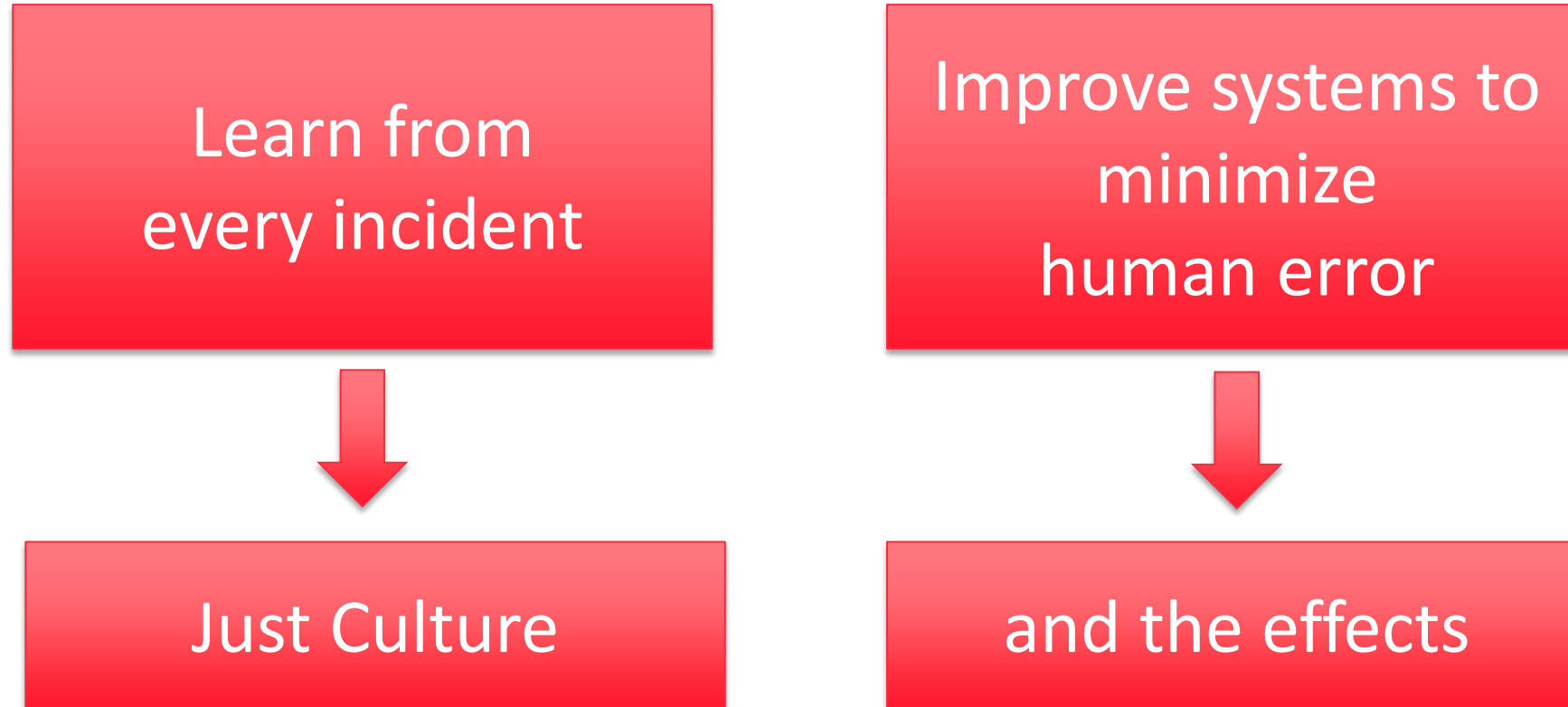
ATC

Engineer

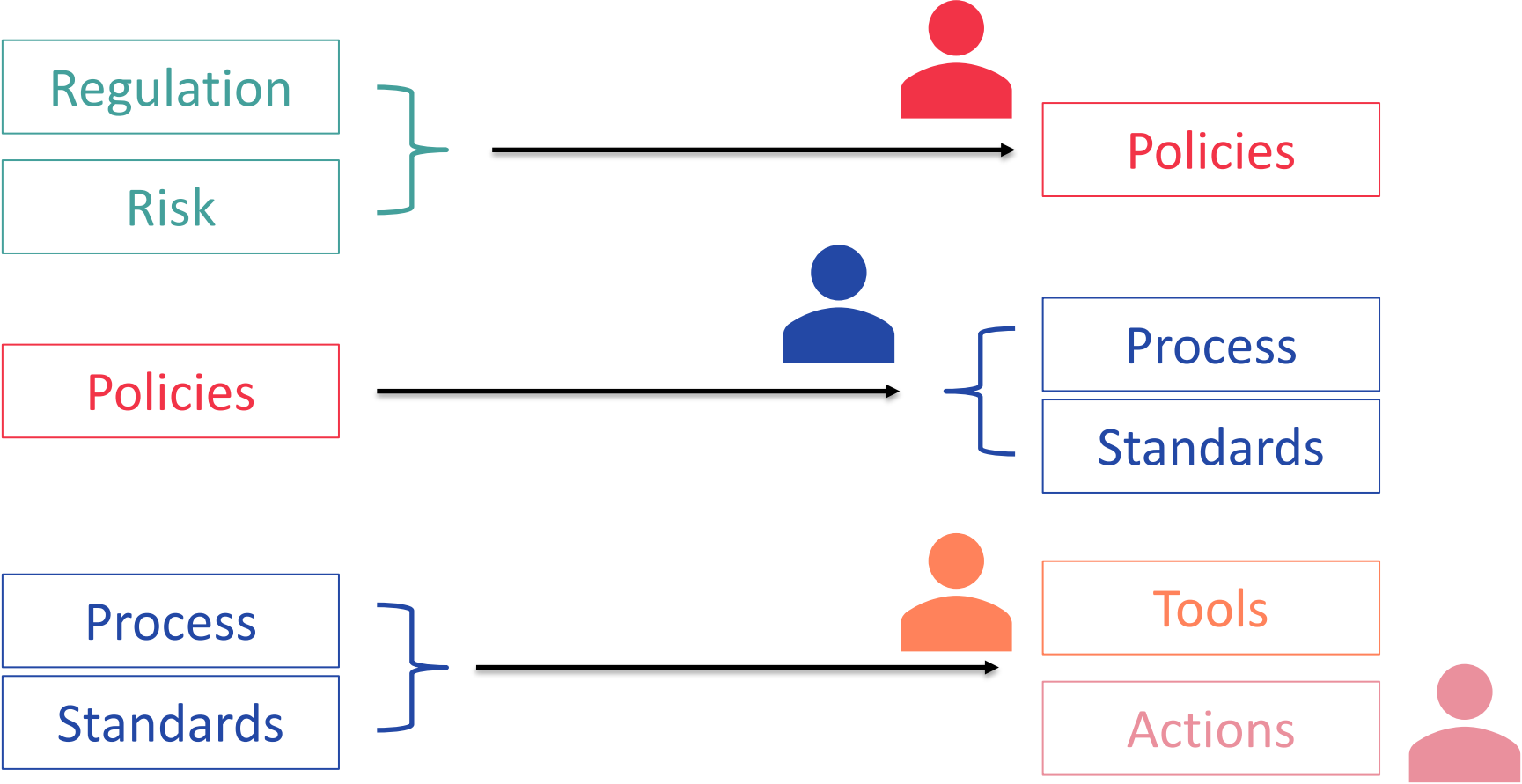
Pilot

Used the risk

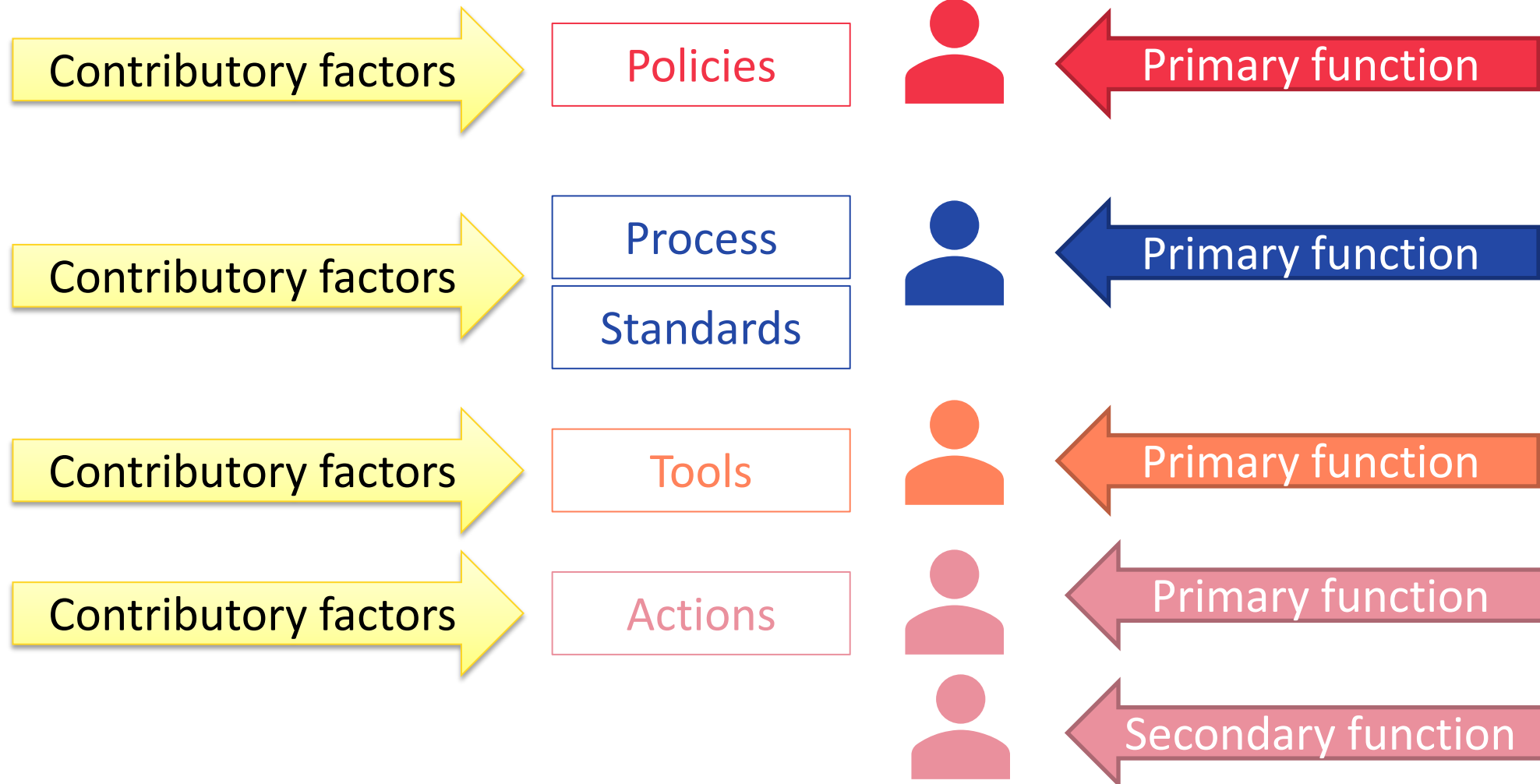
Core approach



Security directives



When there is an incident



RSA[®]Conference2022

What is a Just Culture?



It's about how you deal with this

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Humans make mistakes



- A Just Culture expects mistakes
- Genuine mistakes are not sanctioned, just understood

It's about how you deal with this

Genuine mistakes

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Reckless behavior

It's about how you deal with this?

Because you need
honest answers for your
contributory factor
analysis

Three questions

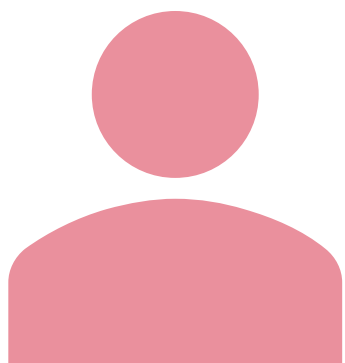


1. Was the
system
designed for
success?

2. Did the
colleague do
what they
should?

3. Did
managers
do what they
should ?

Scenario



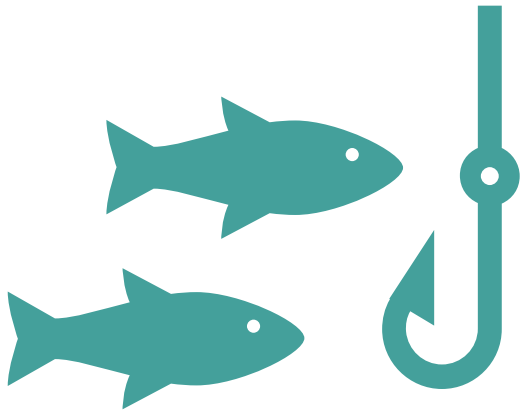
- A new hire (Alice) clicked on a phishing link in an email and both entered her credentials and then downloaded an infected document that installed a RAT on her computer.

What was the cause of the incident?

Human
failure?

Systems
failure?

Contributory factors



- Alice hadn't yet completed her anti-phishing training
- The email passed email filter
 - But other users had reported it
- No link scrubbing in place
- Anti-malware not updated on new laptop

Human failure?

Systems failure?

Systems failure?

Systems failure?

Alice: Three questions

1. Was the
system
designed for
success?

2. Did the
colleague do
what they
should?

3. Did
managers
do what they
should ?

Alice: Three Questions

1. Was the
system
designed for
success?

Contributory Factor Analysis

Alice hadn't been trained

The phish wasn't picked up by the filter

The phish wasn't removed from her inbox

(There was no link scrubber)

The malware solution wasn't configured properly

Contributory factors

Alice's training

Passed filters

No link
scrubber

Anti-malware
not updated

- Policy: Three months from start
 - Follow-up inconsistent
- Alice's manager – Martin – dismissive
 - “Doesn't matter, get on with your job”

Why didn't Alice do what she should?

Didn't register
the risk

Misinterpreted
the risk

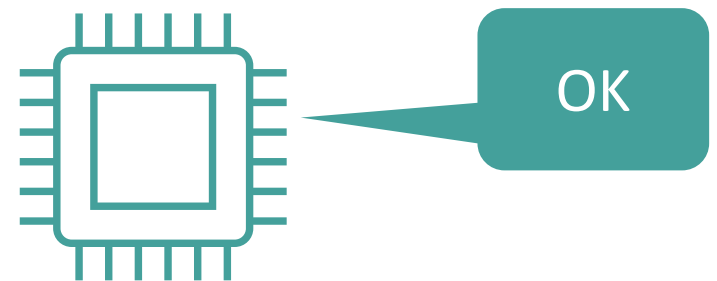
Ignored
the risk

Maliciously
used the risk

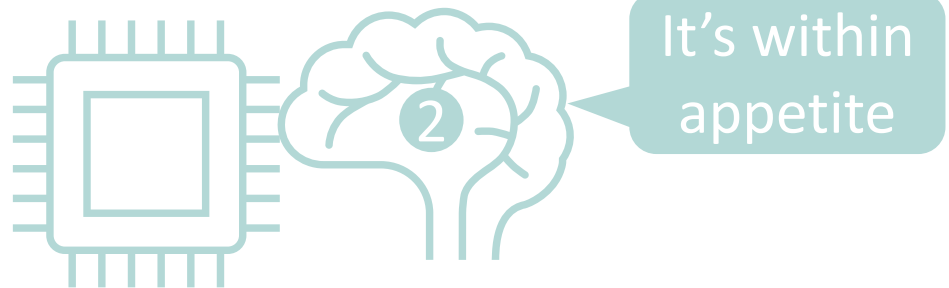
Why didn't Alice do what she should?

Didn't register
the risk

Why didn't Alice do what she should?

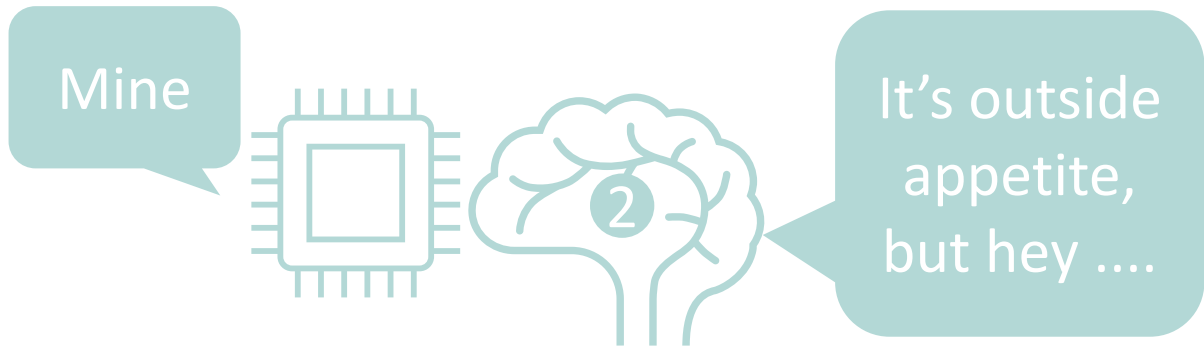


Mine



Didn't register the risk

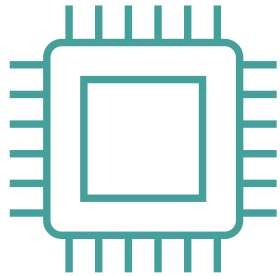
Misinterpreted the risk



Ignored the risk

Maliciously used the risk

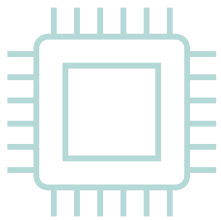
Why didn't Alice do what she should?



OK

Didn't register the risk

Mine



It's outside
appetite,
but hey

Ignored the risk

Analysis

Alice's risk monitor did not register the risk because it had not been trained.

Action

Console Alice 

Train new hires in the first week 

Why didn't Martin do what he should?

Didn't register
the risk

Misinterpreted
the risk

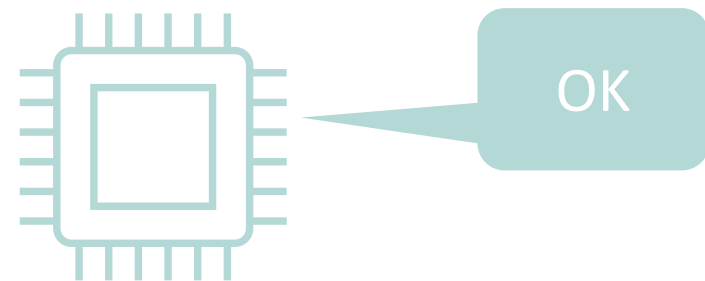
Ignored
the risk

Maliciously
used the risk

Why didn't Martin do what he should?

Misinterpreted
the risk

Why didn't Martin do what he should?

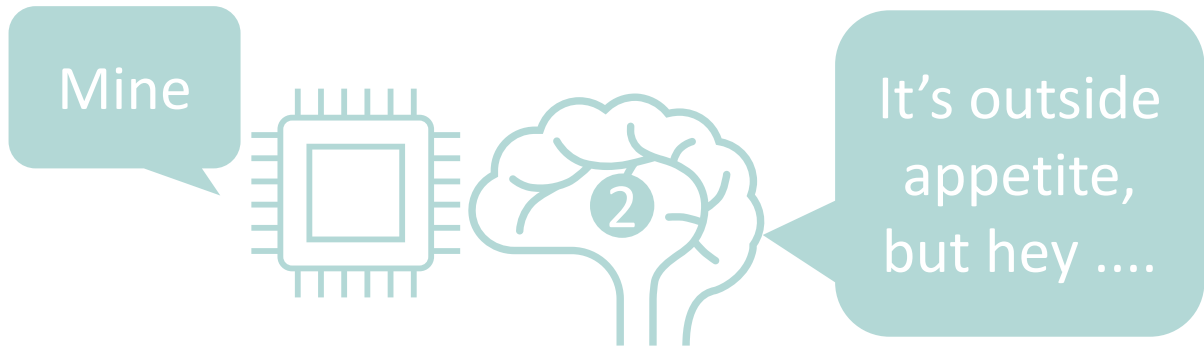


Mine



Didn't register the risk

Misinterpreted the risk



Ignored the risk



Maliciously used the risk

Why didn't Martin do what he should?

Analysis

Martin's risk monitor didn't register the risk of Alice not being trained because:

1. He didn't really understand the risk
2. There traditionally hadn't been follow-up when people missed training deadlines
3. The department is busy

Action

Coach Martin and all managers about the importance of their new hires doing

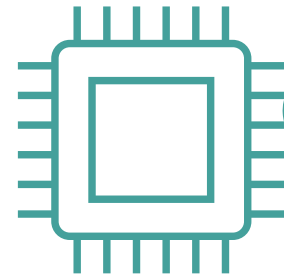


training as soon as possible

L&D will follow up and keep better logs



Mine



It's within appetite



Misinterpreted the risk

Welcome to my devious plan



Maliciously used the risk

Contributory factors

Alice's training

Passed filters

No link
scrubber

Anti-malware
not updated

- Supplier reported filters started picking it up after 12 hours
- Reports of the same phish from other users were in SOC queue
 - Too many tickets, not actioned for 24 hours (breach of policy)
 - This has been the case for 4 months, SOC is 2 FTE under-resourced
 - Steve (relatively new SOC Manager) did not escalate or prioritize recruitment because he was OK with the queues, they are just like his old company and nothing bad happened there

Why didn't Steve do what he should?

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Why didn't Steve do what he should?

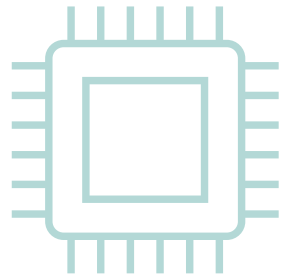
Misinterpreted
the risk

Ignored
the risk



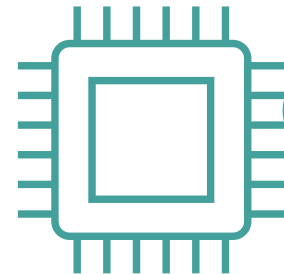
Was Steve
reckless?

Why didn't Steve do what he should?



OK

Mine

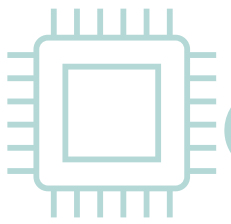


It's within appetite

Didn't register the risk

Misinterpreted the risk

Mine



It's outside appetite, but hey

Ignored the risk



Welcome to my devious plan

Maliciously used the risk

Why didn't Steve do What He Should?

Analysis

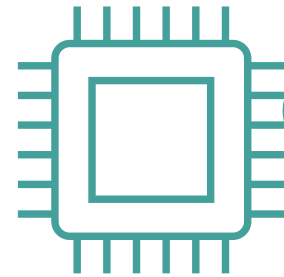
Steve misunderstood the risk of not getting the resource in place so the SOC could follow policy and follow up on phishing tickets.

Action

Coach Steve 
Steve's line manager to play closer
attention to unfilled vacancies 
Is there a governance process missing?



Mine



It's within
appetite

Misinterpreted the risk



Welcome to
my devious
plan

Maliciously used the risk

Contributory factors

Alice's training

Passed filters

No link
scrubber

Anti-malware
not updated

- Sarah (CISO) made a policy decision based on risk assessment and cost
- Not required by any regulatory / legal / contractual reasons
- Approved by annual risk committee

Why didn't Sarah do what she should?

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Why didn't Sarah do what she should?

Analysis

She did everything expected.

Risk analysis informed policy

Policy agreed by appropriate governance structure.

Action

Review risk analysis for a link scrubber

Bring to appropriate governance structure



Contributory factors

Alice's training

Passed filters

No link
scrubber

Anti-malware
not updated

- Laptop deliberately added to wrong group by Bob when preparing Alice's laptop
 - This group doesn't get malware updates
 - Speeds up provisioning by 2 hours
 - Bob wanted to leave early as he was going on holiday that evening, and this was the quickest way of getting the laptop off his desk

Why didn't Bob do what he should?

Didn't register
the risk

Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Why didn't Bob do what he should?

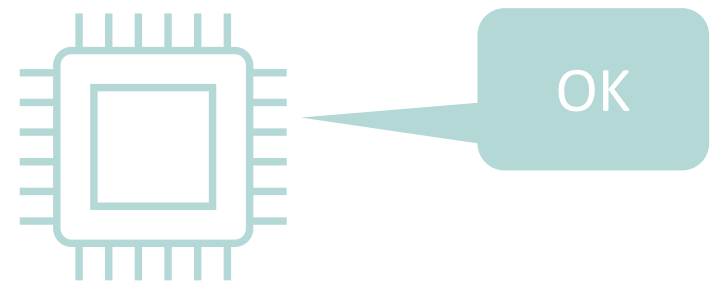
Misinterpreted
the risk

Ignored
the risk



Was Bob
reckless?

Why didn't Bob do what he should?

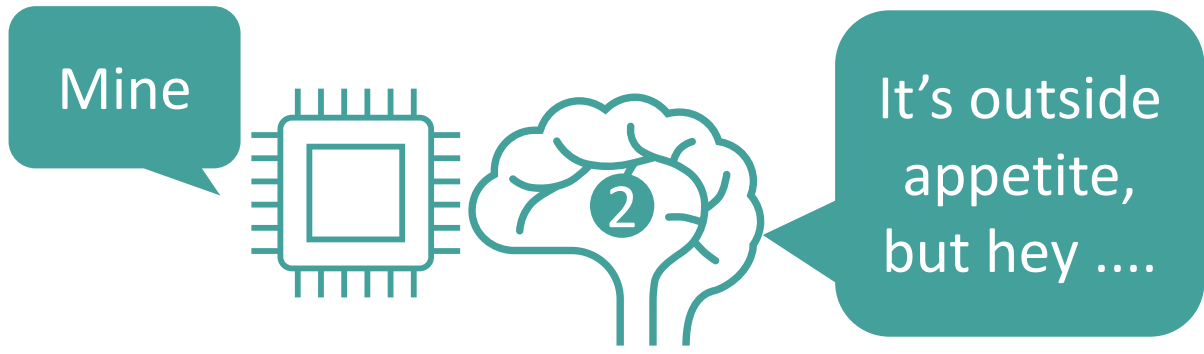


Mine



Didn't register the risk

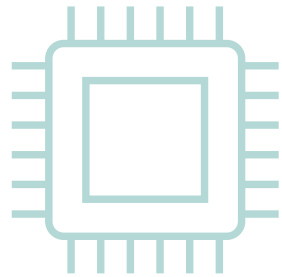
Misinterpreted the risk



Ignored the risk

Maliciously used the risk

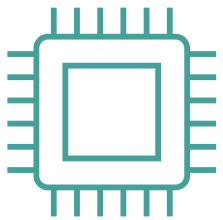
Why didn't Bob do what he should?



OK

Didn't register the risk

Mine



It's outside
appetite,
but hey


Ignored the risk

Analysis

Bob was focused on leaving early to start his holiday and picked the quickest option. There's no guarantee that the anti-malware solution would have picked up the RAT.

Action

Sanction Bob. 

Consider technical controls to prevent systems without anti-malware connecting to user segments. 

Evaluate if the "no anti-malware" group is still needed. 

Just Culture is about how you deal with this

Genuine mistakes

Didn't register
the risk

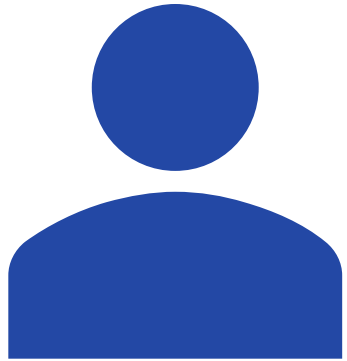
Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Reckless behavior

No harm, no fault?



- Bob argued that the RAT was so new, that even if he had configured the laptop properly, the anti-malware solution still wouldn't have picked up the RAT. So he wasn't part of the problem.

No harm, no fault has no place in a Just Culture.
It encourages risk-taking outside of appetite

What was the human error?

Genuine mistakes

Didn't register
the risk

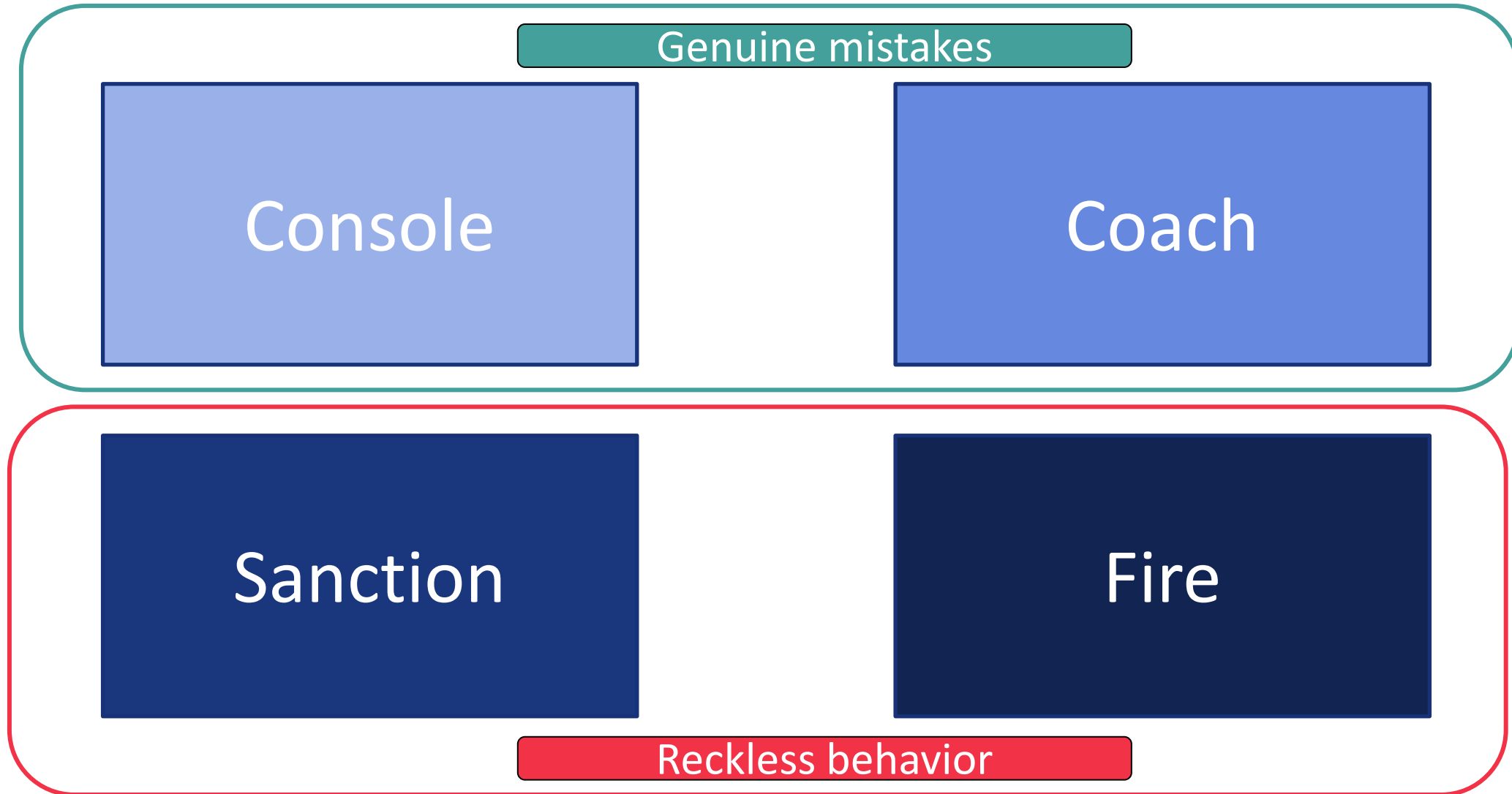
Misinterpreted
the risk

Ignored
the risk

Maliciously
used the risk

Reckless behavior

This is what to do



Actions not Outcomes

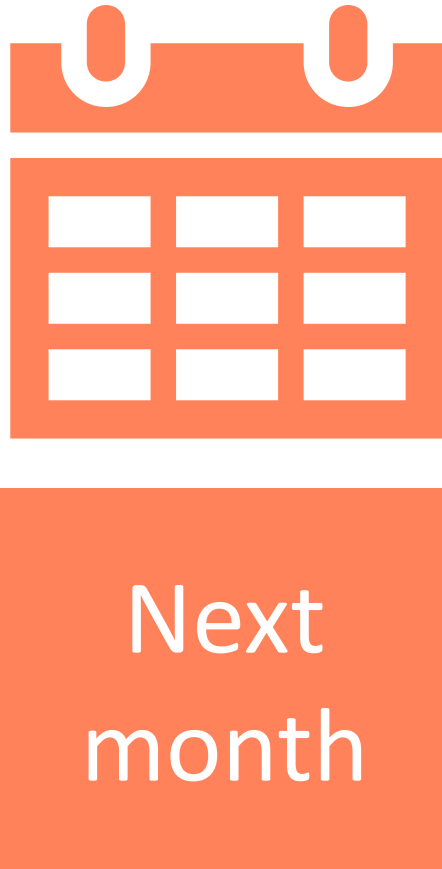
No harm, no fault has no place in a Just Culture.
It encourages risk-taking outside of appetite

What now?



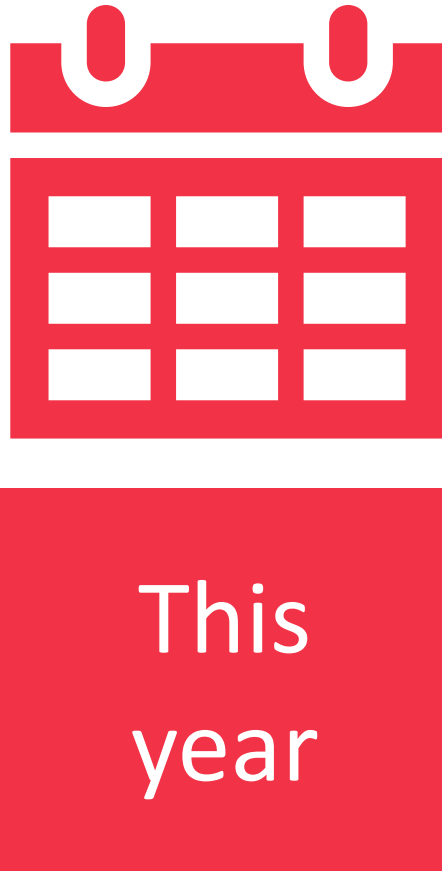
- Look at the culture in your organization?
- Is it a Just Culture?
- Take this scenario, what would your organization have done about:
 - Alice
 - Martin
 - Steve
 - Sarah
 - Bob
- Would the Actions have been the same?
 - People
 - Systems

What now?



- Would implementing a Just Culture improve your information security?
 - Do you have capacity for this?
- What would need to change to implement a Just Culture?
 - Who would need to be onboard?
 - Who could lead this?
 - You need a senior champion
 - Will you be able to get commitment

What Now?



- Internal communications
 - Consistent
 - Everyone onboard
- Change the post incident response to look at contributory factors
- Training of analysts in the methodology
- Peer review of the analysis and actions
- Rigorously track actions
- Evaluate

Read Dave's Subs



A NOVEL STORY ABOUT
WORKPLACE ACCOUNTABILITY

BY

DAVID MARX

AUTHOR OF *WHACK-A-MOLE: THE PRICE WE PAY FOR EXPECTING PERFECTION*

BY YOUR SIDE STUDIOS

AND, YES, THIS IS A BUSINESS BOOK

“The Phoenix Project for Just Culture in Organizations”

John Elliott, RSA Conference 2022