Beyond the e-learning:

Towards a more sustainable approach to cybersecurity awareness

Rosanne Pouw, SURF

2 June,2026

About me

Rosanne Pouw MSc, MPIM, MBA, CISM, CISSP, CIPM

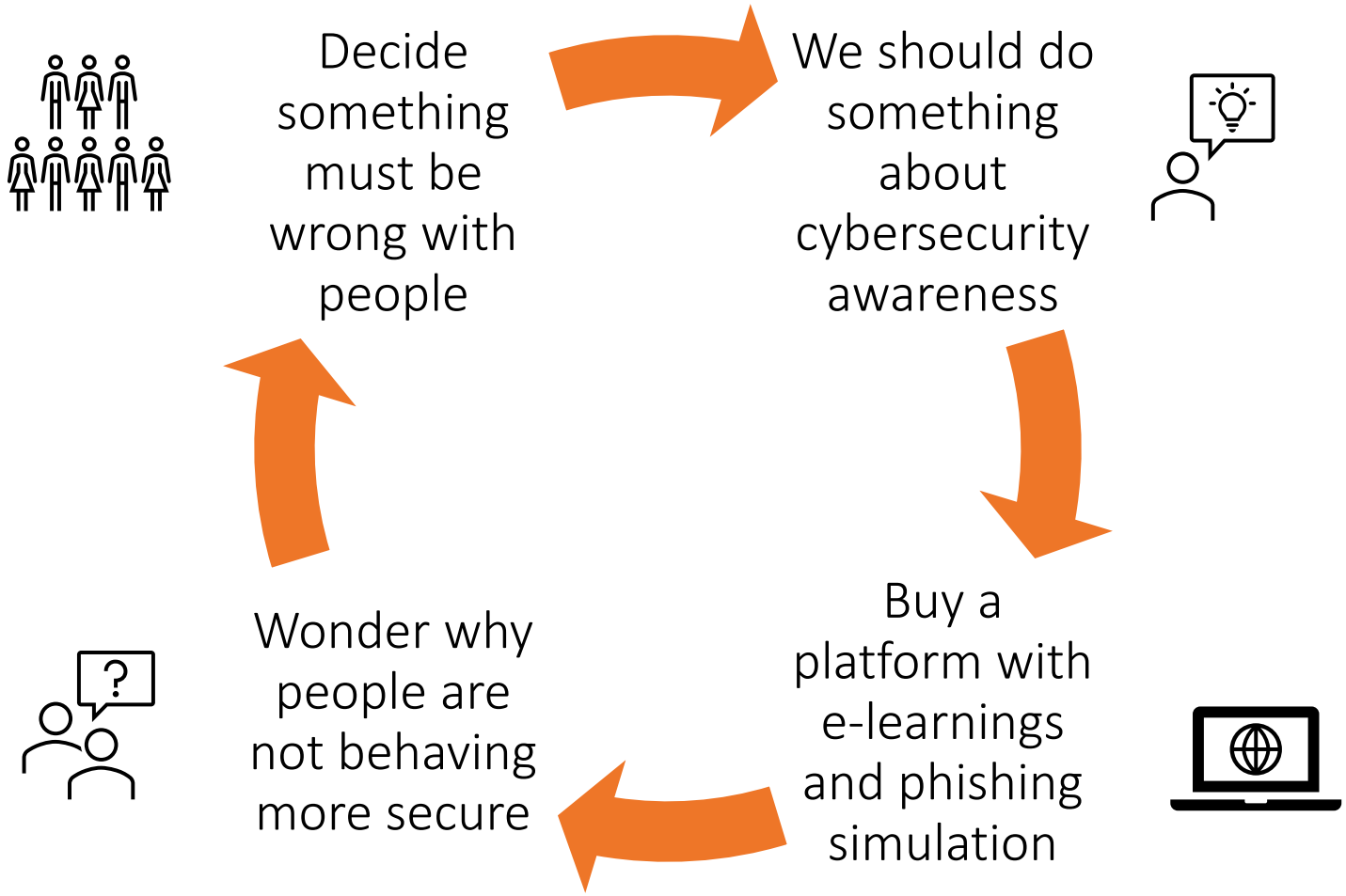
- Social and Organisational Pyschology
- Public Information Management
- Business Administration

12 years - Security Officer & Privacy Officer

3 years - Product Manager Awareness & Training – SURF

SURF: the Dutch National Research & Education Network

The cycle we need to break

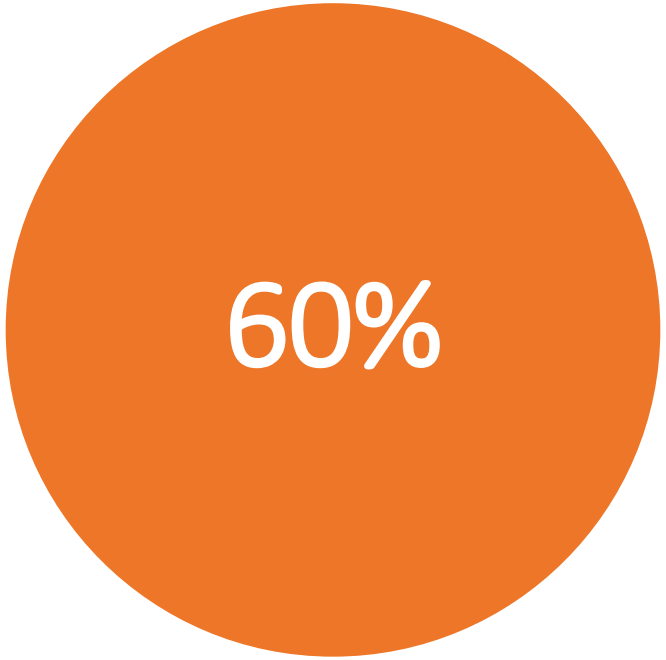


Today’s goal

To give you concrete steps to help you break this cycle

Create a sustainable and effective approach for cybersecurity awareness

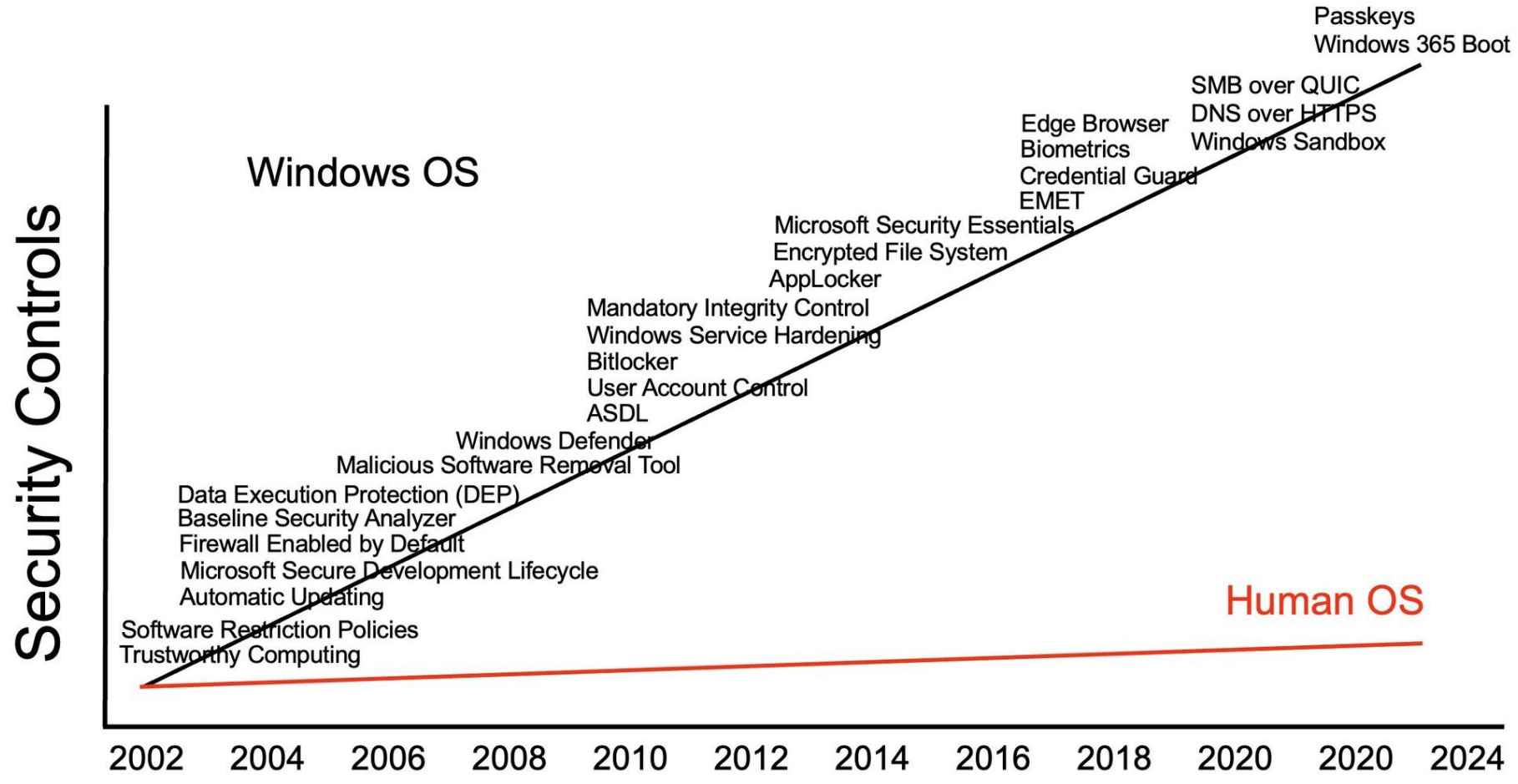
Security incidents and people



People are involved in **60%** of all breaches

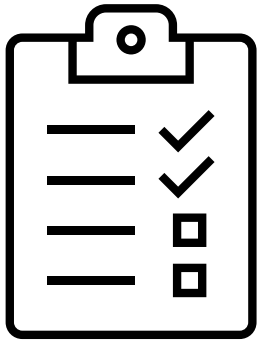
- Verizon Data Breach Investigation 2025

Why are humans a target?



Source: Lance Spitzner, SANS

From compliance to behavioural change

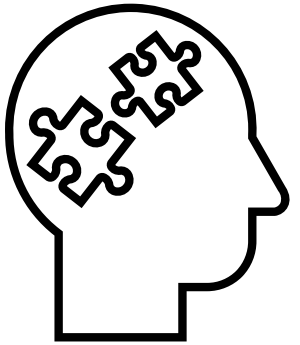


Compliance

Accountability

Proof

Top-down



Behavioural change

Visible change

Resilience

Bottom-up

Examples of compliance based awareness

SURF

Phishing simulations

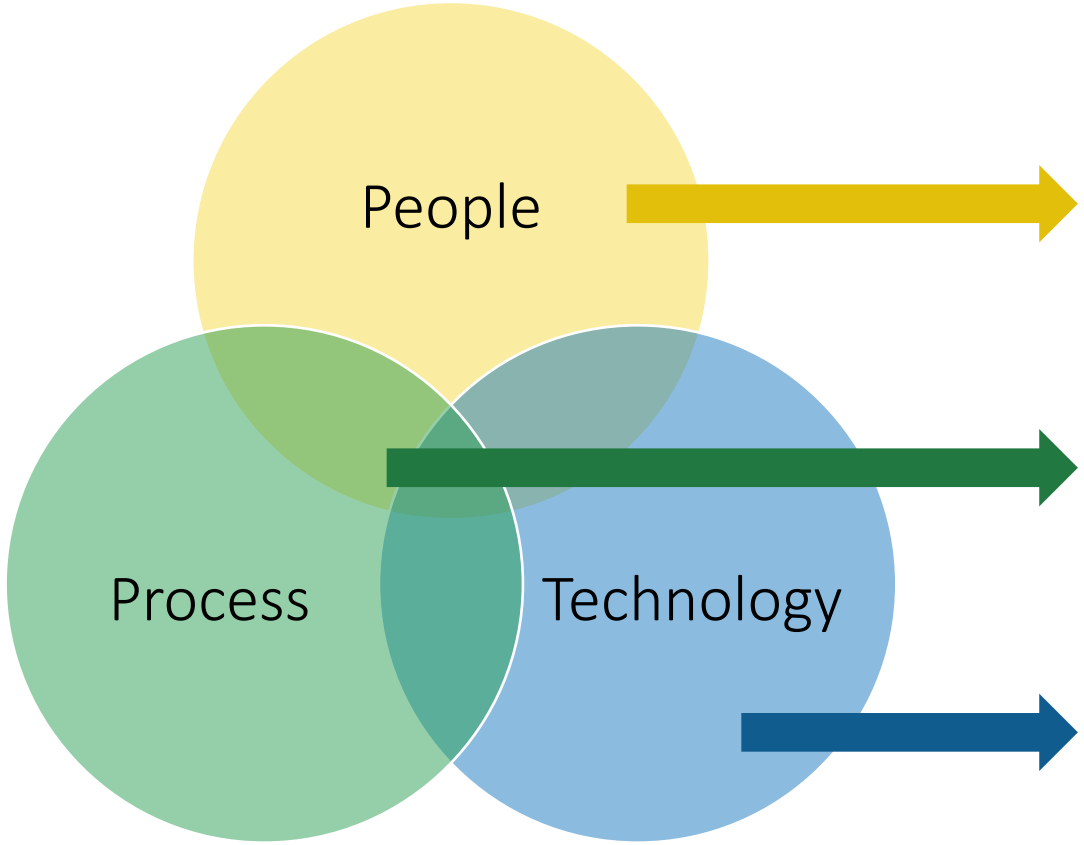
Phishing simulations give insight in:

- how many people click your phishingmail
- How many people report your phishingmail

They don’t offer an insight or explanation why people ignore, click or report

A balanced awareness program can contain phishingsimulation as one of the tools

People, Process, Technology



Risk: phishing

User training & Email reporting

Incident management & Reporting processes

Employ anti-spoofing measures (Including DKIM, SPF, DMARC)

Full phishing treatment plan:
https://www.ncsc.gov.uk/guidance/phishing

CYBER SAFETY: ONLINE SAFETY AND PRIVACY

Home Cyber safety
+ Cybersafety
+ Privacy: personal data
News
+ How to protect yourself
+ Recognizing incidents
Report an incident
+ Responsible disclosure
Contact

IMPORTANT ANNOUNCEMENT: MANDATORY PRIVACY AND SECURITY AWARENESS TRAINING

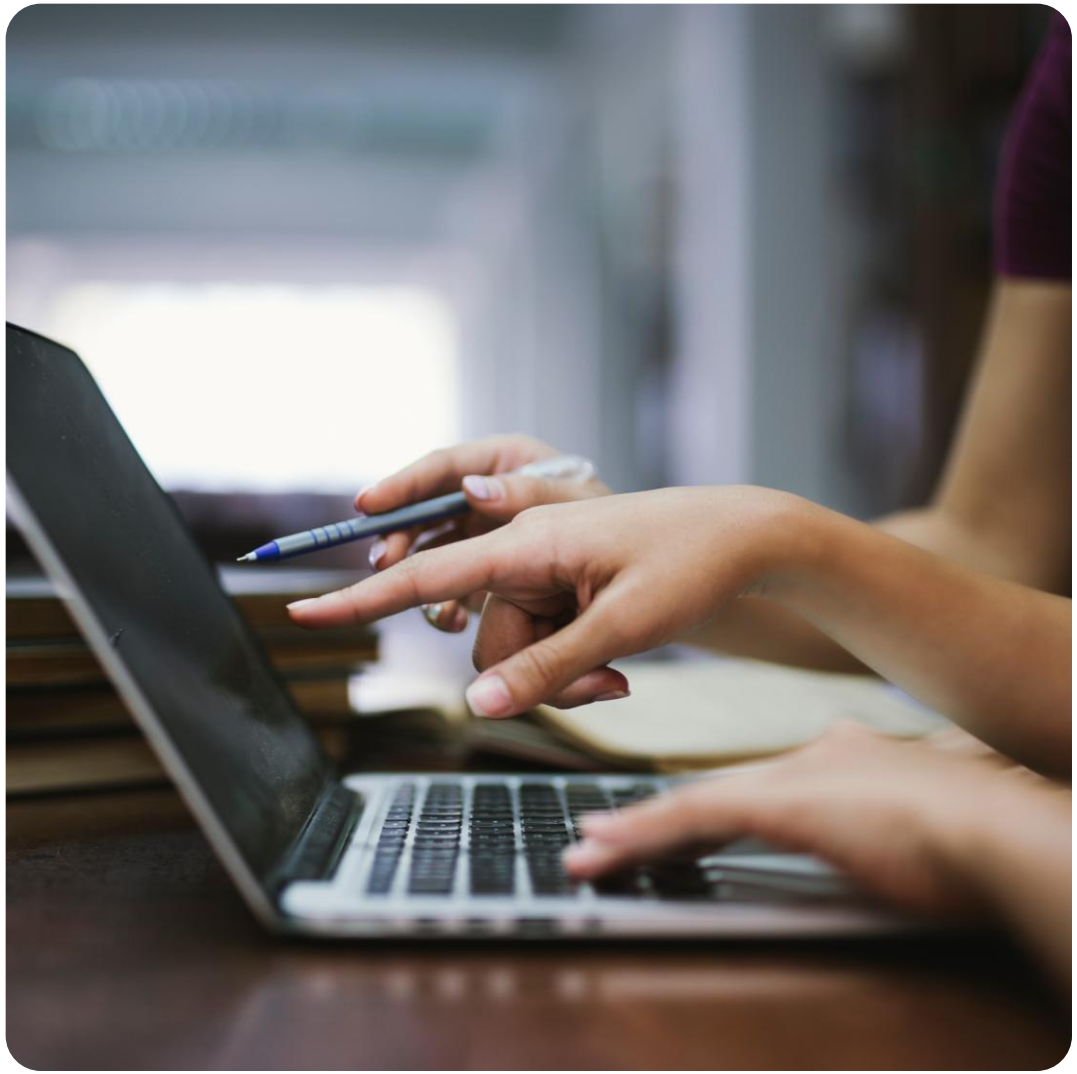
Sunday 17 March 2024

Mandatory training

Gives insight in percentage of employees that finished a training

Measures knowledge (quiz or test)

But does it change the behaviour of employees?

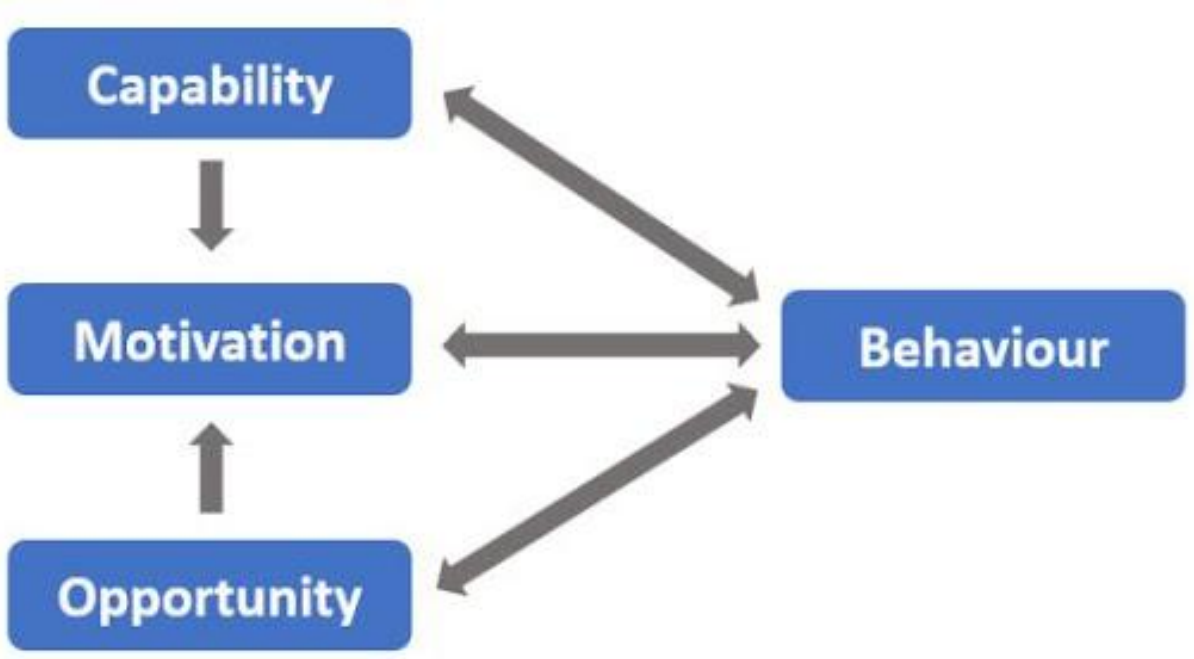


COM-B model

Is the person capable ? Did they receive training and posess the knowledge and skills to recognize phishing mail?

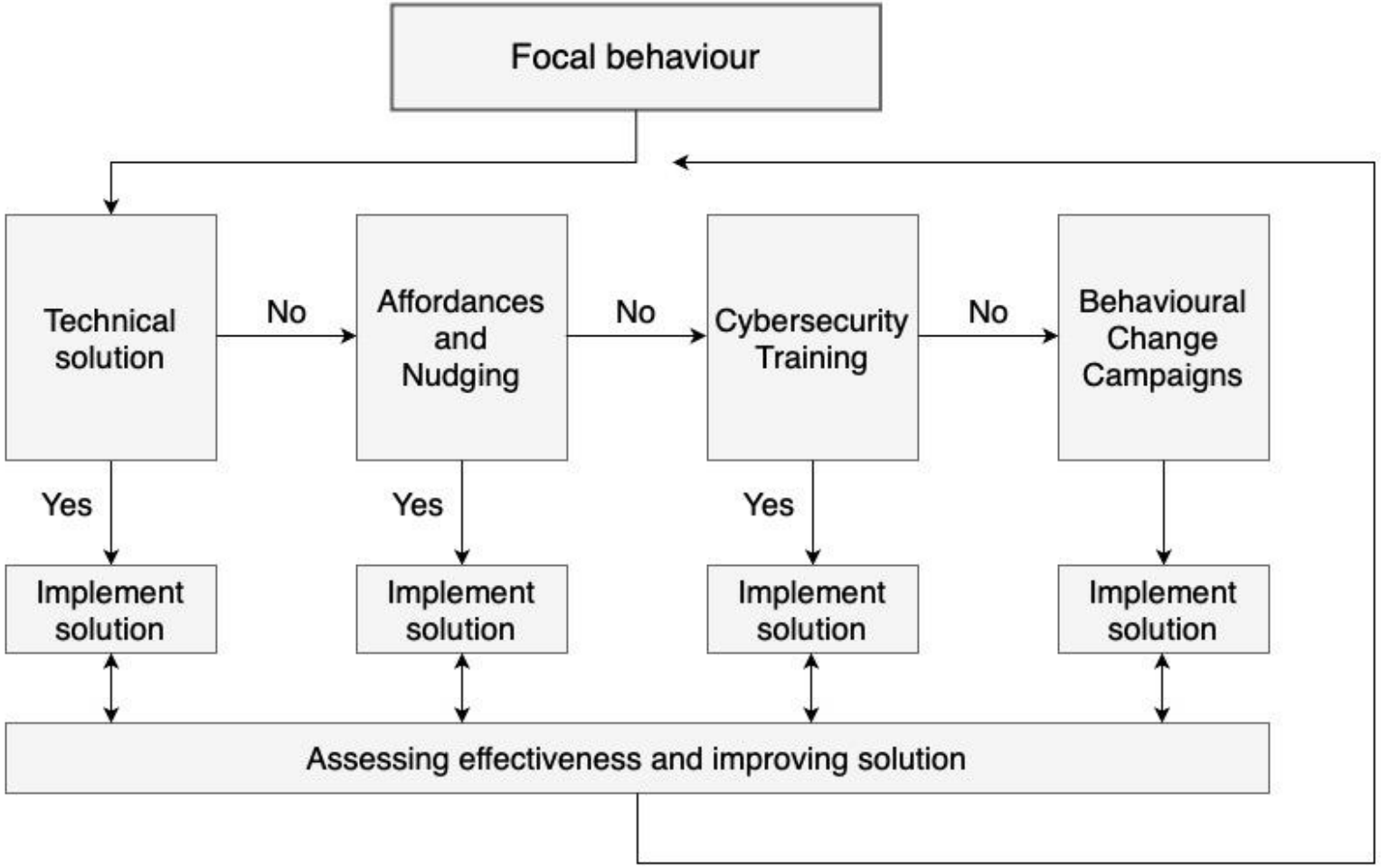
Is the person motivated? Do they believe it is important and useful to report phishing mail?

Does the person have an environment that supports this behaviour? Is reporting phishing mail appreciated? Is it easy to report a phishing mail with a button?



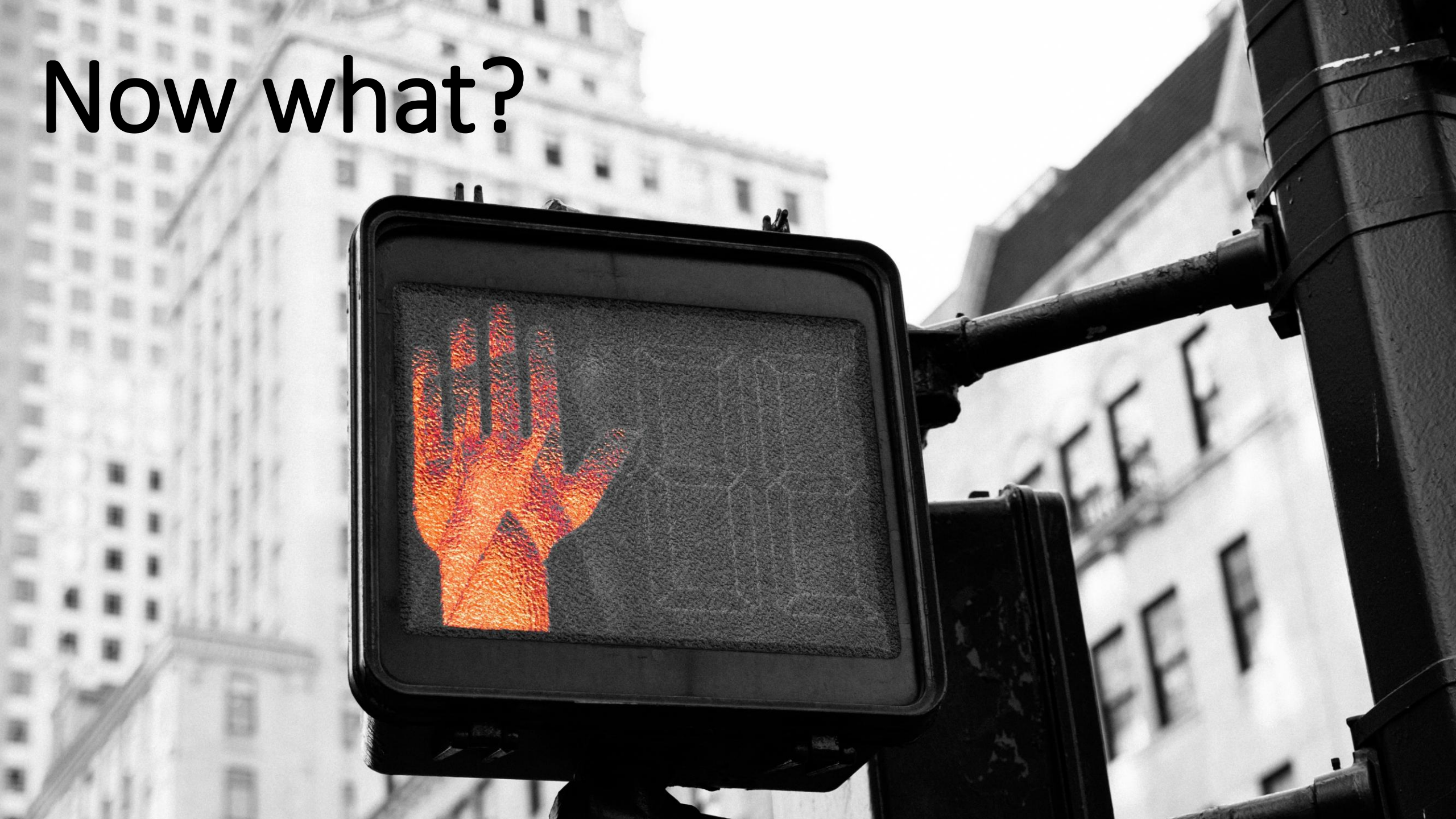
COM-B model, Michie et al 2011: https://www.behaviourchangewheel.com

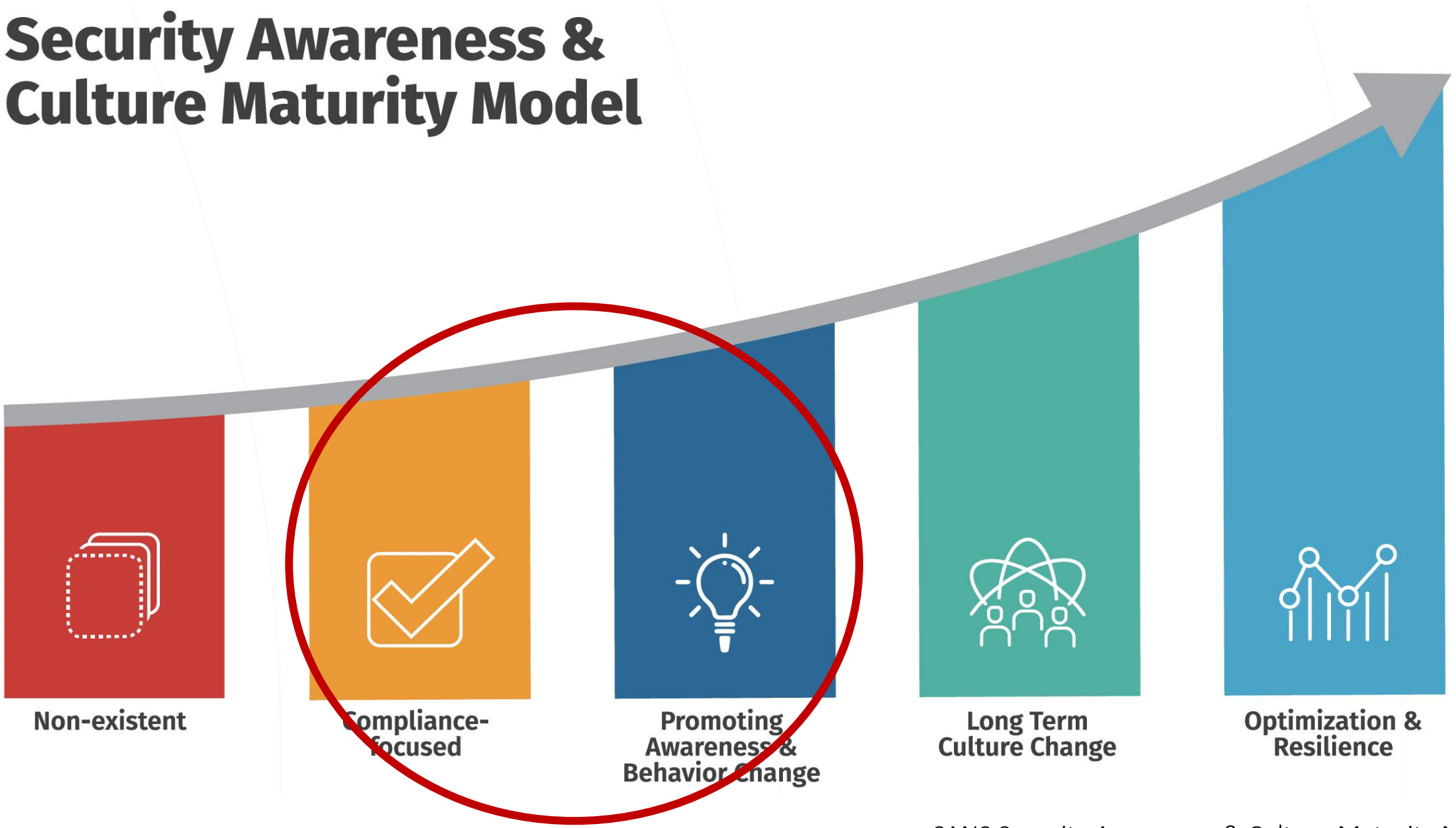
Changing behaviour through training



https://www.universiteitleiden.nl/en/research/research-output/governance-and-global-affairs/developing-a-behavioural-cybersecurity-strategy-a-five-step-approach-for-organisations

Now what?





SANS Security Awareness & Culture Maturity Model

Awareness as a process

Awareness is not a quick fix

Start looking at cybersecurity awareness as a process

A cycle that helps you change behaviour

What are your risks?

What behaviour do you want to change?

People, Process, Technology Behaviour change model

Create a cohesive programme

Commitment from the board
Manage stakeholders

Support from other departments

Evaluate your whole program

SANS Awareness Maturity Model

What would you change in the next cycle?

Involve educational expert

Use tools that support your programme plan

Measure effectiveness
Evaluate activities

Concrete tips

Think outside the (cybersecurity) box: multi-disciplinairy approach

Don’t know where to start? Start with risk management!

You need everyone inside your organisation to contribute

Use recent insights from scientific research to improve your program

Small steps lead to big changes

Want to read more?

Find more info on the structured approach for awareness in the GÉANT Wiki

GÉANT Article: **Inside PDCA: a practical framework for sustainable cybersecurity awareness**


Thank you for your attention!
Rosanne.pouw@surf.nl
SURF